Employee Surveillance: The Road to Surveillance is Paved with Good Intentions

Lilian Edwards, Laura Martin and Tristan Henderson[1]

Introduction

Privacy in the workplace has for many years been a contested concept, with traditional ideas that a worker cedes personal autonomy and rights as a natural consequence of entering the employment sphere,[2] coming into conflict with more modern ideas, especially in Europe, that workers remain humans with rights, albeit possibly limited, in the workplace, and that in the long-hours culture that now rules many workplaces, a degree of sympathy for private life and self-fulfilment must be retained.[3] At a time of expanding state and private sector surveillance,[4] the modern workplace has also become a key site of surveillance technologies, with ever cheaper monitoring tools used pervasively, including audio and video surveillance, interception of calls, e-mails and web traffic, and more recently "smart" tagging of workers' desks, cars, lapel badges, door passes, phones et al to measure location, activity and productivity; and algorithmic profiling to derive intelligence feeding into, and sometimes altogether determining without human input, hiring, firing and promotion decisions. Employee surveillance long precedes technological innovation, of course. Human surveillance of the direct kind, unmediated by technology (for example, shop floor or factory managers patrolling by eye) still occurs in contemporary society, although it is often now combined with technological tools. Information technology has transformed the nature and extent of surveillance at work by affording employers with remarkable monitoring abilities which go beyond the localised workplace to extend to the home and social environment, and pervasively surveille not just conventional work hours but 24/7.[5] In our work we trace the history of employee surveillance at work through the lens of dominant technologies of each era. A novel five-phase model of surveillance is proposed:

- Surveillance 1.0 - physical and analogue surveillance;
- Surveillance 2.0 - databases and dossiers;
- Surveillance 3.0 - digital networked technologies;

[1] Respectively, Professor of E-Governance, Law School, University of Strathclyde; Doctoral candidate, Law School, University of Strathclyde; Senior Lecturer, School of Computer Science, University of St Andrews.
[2] See Kahn-Freud, O. 'The Legal Framework' in Hardy, S.T. *Labour Law in Great Britain*, Fifth Revised Edition (England: Kluwer Law International: 2012)
[3] *Niemietz v Germany* [1992] ECHR 80
[4] For an overview and some insights into state surveillance after the Snowden revelations, and surveillance in the private sector by social media, retail, marketing and Internet industries, L Edwards *Law, Policy and the Internet* (2018, Hart Publishing) chs 5-7.
[5] Ball, K. 'Workplace Surveillance: An Overview' (2010) Labor History, 51(1), pp87-106

- Surveillance 4.0 - connected smart devices and the Internet of Things;
- Surveillance 5.0 - big data and algorithmic profiling and classification

Regulation has responded to, or is in the process of responding to, the technologies in each of these phases and their effects on worker and workplace privacy, albeit sometimes more slowly than is desirable. The right to respect for private life has been asserted as applicable to the workplace in a series of Strasbourg cases beginning in 1992.[6] However, employee surveillance, as in so many areas of technology, at the moment outpaces law, and algorithmic profiling of the workplace in particular is so far an understudied area where worker rights are coming under potential threat. This is particularly true in the so-called "gig" economy, where typically systematic use of precarious "zero hour" contracts not awarding full employment rights, has intersected with ever closer micro-surveillance, assisted often by use of "smart" or "Internet of Things" technologies (think Amazon's workers, speed tested as they move around warehouses, or Uber's drivers, remotely monitored by the location data their cars collect along routes and the ratings their passengers give them.) In short, workplace surveillance has become a perfect storm of convergence of surveillance technologies with results that are under-anticipated by regulation and, via scope creep, have the potential to seriously impair the rights of employees. While our five-phase model is a step forward in analysing the rise of automated workplace surveillance, what also became noticeable in our research is that earlier technologies can be co-opted into newer models of surveillance, with results that are under-anticipated by regulation and, via scope creep, have the potential to seriously impair the rights of workers.

Accordingly, we present a fortuitous case study with which two of the authors have been closely involved. The academic (UCU) strike action in the UK in 2017-2018 threw up a highly combative environment where some universities reportedly considered or attempted to "strike break" by replacing, without new permission or consent, striking academics with recordings of their lectures made in previous years. These recordings were usually made for laudable motivations such as widening access and allowing students to revise. On examination, this practice of mandated lecture capture, unchallenged when used to help students but now under examination when its use is transformed, is often of dubious legality, both with reference to copyright[7] and data protection, as well as overarching privacy rights and the relationship of trust and confidence between employee and employer. Furthermore,

[6] *Niemietz*, sura n 3

[7] In this paper, we concentrate on the privacy and surveillance dimensions, though the copyright issues are certainly worthy of future work.

evidence is emerging that some universities are without publicity using lecture capture as a surveillance mechanism to grade or intimidate academics, or as a means to covertly replace them entirely. Serendipitously a recent European Court of Human Rights (ECtHR) case, *Antović and Mirković v Montenegro*[8] provides some ammunition with which to dispute these transformative and unsettling re-uses of recorded lectures.

Finally, we consider the negative consequences of such non-permissioned re-use, which may include not just breach of trust placed in university management by academics, but withdrawal from positive uses of lecture capture such as widening participation and enabling access, as well as loss of trust by students in their university management. We make some recommendations, including that lectures should never be recorded without explicit consent to processing of personal data and that recorded lectures should never be re-used for non-core educational purposes without explicit consent. Ideally these recommendations would be incorporated into guidance such as the recently revised JISC guidance for universities. Finally we consider if the UCU strike case study has wider implications for the evolution of surveillance in the wider world beyond academe.

A history of workplace surveillance and technology; the five phase model

Surveillance 1.0: analogue world

Physical oversight and analogue recording of employee activity exemplify Surveillance 1.0; the first foundational phase of employee surveillance. Business historians report that extensive monitoring of the workforce was adopted as a means of control in early 20th century manufacturing factories.[9] The 'panoptic' physical architecture of the workplace permitted extensive and intensive visual oversight of workers undertaking their duties.[10] Foucault notes that "by walking up and down the central aisle of the workshop, it was possible to carry out a supervision that was both general and individual".[11] In the latter half of the 20th century employers' physical surveillance capabilities were supplemented by management theory and testing techniques. Fredrick Taylor's *Principles of Scientific Management*[12] attempted to

[8] Application no. 70838/13, 28 November 2017; [2017] ECHR 365.

[9] Landes, D. *'The Unbound Prometheus: Technological Change and Industrial Development in Western Europe from 1750 to the Present'* (Cambridge: Cambridge University Press, 1969)

[10] See Bentham's infamous 18th century panopticon prison design. Bentham, J. '*An Introduction to the Principles of Morals and Legislation'* (1780) Reprinted by Dover Philosophical Classics (NY: Dover Publications Inc, 2007)

[11] Foucault, M. *'Discipline and Punish: The Birth of Prison'* translated by Sheridan, A. (New York: Vintage Books, 1991)

[12] Taylor, F.W. '*The Principles of Scientific Management'* (NY: Harper & Bros, 1911) {WWW Document} http://public-library.uk/pdfs/8/917.pdf (visited 14 July 2018)

improve workforce efficiency by enabling high levels of managerial control over the employee in the course of his working duties. Fragmentation of tasks, close visual observation and timing of every aspect of job execution were undertaken in order to assign employees to the most suitable tasks and to allow employers to specify "not only what is to be done but how it is to be done and the exact time allowed for doing it".[13] Furthermore, surveillance techniques began to dominate selection, promotion and firing as employers adopted psychological, genetic and physical testing in attempts to uncover employee ability and aptitude.

Surveillance 2.0: database nation

By the late 1970's policymakers were exhibiting significant concern about Surveillance 2.0, involving computer automation, digitisation of files and the creation of data banks.[14] Surveillance had become built into the infrastructure of the workplace as computers continuously generated, captured and processed data on a scale unprecedented in the analogue era. Intensive digital monitoring could now be undertaken as it was possible to track the employees' every interaction with computer equipment and software. Recording of *inter alia* keyboard activity, application usage and mouse clicks provided employers with comprehensive overviews and intensive insight into employee activity. One of the most profound aspects of computerisation, however, is the employer's ability to engage in 'surveillance through database'. The database allows for data to be compiled, tabulated, sifted, and cross-referenced instantaneously and more accurately than paper-based analogue techniques. The database presents data in a manner apt for analysis affording employers with extensive oversights, the ability to undertake systematic investigation and comparison of workforce performance whilst being able to uncover individual tendencies, characteristics and behaviours. Sharing of databases allows for the construction of detailed profiles on the individual and grants employers insights into the lifestyles of employees, something fully exploited later in phase 5.0.[15] With computerisation, data can be 'mined' in limitless numbers of useful ways to reveal patterns and produce actionable information.

Surveillance 3.0: the Internet and interception of communications

[13] *ibid.,* Chapter 2

[14] For an overview of UK and European policy discussions on the matter see Kosta, E. *'Consent in European Data Protection Law'* (Leiden: M.Nijhoff Publishers, 2013) ch 2; for a US perspective on the rise of private and public database keeping, see D Solove '*The Digital Person'*, (NYU Press, 2004) ch 1.

[15] See Garfinkel, S. 'Database Nation: The Death of Privacy in the 21st Century (Cambridge: O'Reilly, 2000) and Lyon, D. '*Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination'* (London: Routledge, 2003)

From the mid-90s on, the Internet, as it became a vital tool for work, enabled a new type of surveillance via the interception of worker communications. This Surveillance 3.0 allowed employers, at a distance and with minimal effort, to track employees' entire work and sometimes home life via their calls made, e-mails sent and online sites visited. The integration of the Internet into the workplace and its unauthorised use by employees at work presents justifiable concerns to employers in terms of fears of slacking, misuse and illegal behaviour for which the employer might be liable (eg downloading of obscene material, defamation of others) and as a result software enabling real-time recording of communications and online activities became standard. Crucially though, many employers can thus now gain insight via communications and browsing histories into not just the labour of their workforce, but also their personal relationships, thoughts, opinions, preferences and interactions.[16] Employers can also gain unprecedented insight into the lifestyles and non-work activities of employees through identifying *inter alia* social media accounts and personal blogs, and sometimes, demanding password access to these.[17] As our online lives have become arguably as important as our offline ones, these developments have severely prejudiced not just worker but personal privacy and may also affect the friends and family of workers.

Surveillance 4.0: smart tech, ubiquitous computing and the Internet of Workers

Although surveillance of the worker in the real world has always been possible (see phase 1.0), it was limited by practical constraints. Every worker could not easily be physically monitored by humans all day and not at all outside the physical work area. Workers inevitably outnumbered supervisors, Bentham's Panopticon not being generally a real architectural phenomenon. Pervasive information technologies such as CCTV and RFID tracking began to make inroads into this uneven power balance as early as the 1970s (CCTV) and 1990s (RFID) and became, the former especially, standard parts of employee surveillance. However, these technologies have now been subsumed within and extended by a more powerful wave of real world surveillance technologies: the Internet of Things (IoT).[18]

[16] ECtHR cases have revealed the extent of insights employers have gained through this type of surveillance. For example, see *Copland v The United Kingdom* [2007] ECHR 253 and *Barbulescu v Romania* [2017] ECHR 754.
[17] In the UK the ICO has warned that such a practice might be a breach of data protection rights, whereas it is relatively common in the US: see "Employers warned against demanding Facebook details from staff", Guardian, 26 March 2012 at https://www.theguardian.com/technology/2012/mar/26/employers-warned-facebook-login-details .
[18] There are inconsistencies and confusion over the definition of the IoT. See Manwaring, K., Clarke, R. *'Surfing the third wave of computing: a framework for research into eObjects'* (2015) Computer Law & Security Review: The International Journal of Technology Law and Practice, 31(5), pp586-603. See discussion of the impact of the IoT generally on user privacy in L Edwards "Privacy, Security and Data Protection in Smart Cities: A Critical EU Law Perspective "(2016) 2 Eur. Data Prot. L. Rev. 28. For the purposes of this paper the

Surveillance 4.0 relates to the real-time, ubiquitous and unobtrusive surveillance of employees made possible by small cheap sensor technology capable of being embedded within the working environment, everyday objects and even the human body. The nature of IoT devices (whether worn or embedded within the environment) allows for intimate 24/7 tracking which gathers data on the everyday reality of employees.[19] Richards notes that with the IoT in the workplace "more and more previously unobservable activity (is subject) to electronic measurement, observation and control".[20] Biological, psychological and emotional surveillance are also facilitated through application of the IoT to the workplace. Interaction with the IoT becomes unavoidable, and often cannot be left at home (especially given the portability of most electronic devices these days, the expectation of employees to be allowed to "Bring Your Own Device (BYOD)"[21] and the dual use of eg taxis at work and home) granting employers real-time insights into employees most intimate moments as well as work activities.

Surveillance 5.0: the age of algorithms

Machine learning (ML) algorithms (often, wrongly, described as "AI") are increasingly being applied to "big data" generated by Surveillance 1.0 to 4.0 (and by other industries such as retail, marketing or social media) to enable further surveillance of the worker. Data analytics algorithms are designed to generally spot patterns in large amounts of data, enabling categorisation and profiling. Applied to the labour market, this enables automated or assisted decision making about hiring, firing and internal promotion or disciplining. Through algorithmic analysis of big datasets, employers can identify behaviours of interest, uncover emotional states, expose unshared personal preferences and even create new knowledge. For example, lip-reading and facial-recognition algorithms applied to CCTV recordings can provide employers with full transcripts of employees' private conversations.[22] Uses of such algorithms are mushrooming as costs fall and data grow. At a most basic level around 90% of workplaces have admitted using Google and social media sites to research a job candidate -

IoT relates to computer processors and networks of sensors capable of data collection, processing and communication and embedded within everyday objects, the physical architecture of the workplace and even the human body allowing for the real-time transmission of data to employers.

[19] A29WP note that the IoT allows for the tracking of "an individual's even more detailed and complete life and behaviour patterns". See A29WP, *Opinion 8/2014 on the Recent Developments on the Internet of Things,* WP 223, p8.

[20] Richards, N.M. '*The Dangers of Surveillance'* (2013) Harvard Law Review, Vol126, 1934-1964, p1940

[21] Weeger, A., Wang, X., & Gewald, H. (2016). 'IT consumerization: BYOD-program acceptance and its impact on employer attractiveness' Journal of Computer Information Systems, 56(1), pp1-10.

[22] See M Veale and L Edwards, "Better seen and not (over) heard? Automated lipreading systems and privacy in public places", EU PLSC, Brussels, January 2018.

something which has been banned in Germany[23] – while at a more sophisticated level, a number of firms now offer services to profile potential or actual employees using every known piece of human resources, performance and appraisal data, every internal communication or web search, customer feedback or rating, enhanced intelligence from CCTV (eg emotional information) and external data such as social media posts or police reports.[24] Algorithms are parasitic on all the preceding surveillance phases, but add new elements of claimed predictiveness which may be confused with actuality, along with dangers of bias, error and discrimination, unfairness and lack of transparency which makes them hard to challenge; these features are now well documented.[25] As such they may be the most dangerous technology yet in the ongoing land-grab for employee privacy.

Lecture capture and repurposing as surveillance: our case study

As the last section showed, technology now affords employers with arguably greater surveillance capabilities than at any time in industrial history. Privacy in the workplace, a value recognised explicitly by the ECtHR, is under severe threat. Surveillance extends beyond the workplace to home and socialising environments, and can be pervasive and 24/7, rather than restricted to constrained working hours and clearly defined work tasks. Every aspect of worker behaviour including location, productivity, attitude and conversations can now be gathered and analysed in "smart" surveilled or intercepted environments or from sources such as social media. Positive behaviour (eg fitness) may be mandated,[26] as well as negative behaviours (eg slacking, theft) reduced. The incursion into private life both in and outside work is profound as well as the private life of friends, families and contacts). Most worryingly perhaps, job acquisition, security and progression may in future be determined wholly or partially by automated algorithmic systems whose frailty in relation to fairness, transparency and accountability[27] is now well recorded. Despite the phase model outlined

[23] Germany has banned employers from searching job candidates on social networks used for electronic communication, except where the site exists to represent the professional qualifications of members. German employers can use search engines and sites such as Linkedin but are forbidden from looking up candidates on Facebook and Twitter.

[24] For example, See https://www.sterlingtalentsolutions.co.uk/ and https://www.veroscreening.com/services/employment-screening/

[25] See eg Edwards, L. and Veale, M. " 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 (2017).

[26] For a discussion of employee surveillance and wellness programmes in the US legal context, see Ajunwa, I., Crawford, K., & Schultz, J. (2017). "Limitless worker surveillance." California Law Review, 105(3), pp735-776.

[27] There has been a large amount of interest in fairness, accountability and transparency for algorithmic decision-making in recent years, as evidenced by the creation of the FAT ML and FAT* stream of conferences – see https://www.fatml.org/. For a general overview of some of the issues, see Kroll, J. A., Huey, J., Barocas, S., Felten, E. W., Reidenberg, J. R., Robinson, D. G., & Yu, H. (2017). Accountable algorithms. *University of Pennsylvania Law Review*, 165(3), pp633-705; Lepri, B., Oliver, N., Letouzé, E., Pentland, A., & Vinck, P.

above, the world is sometimes more complex than consecutive. Older technologies may be co-opted into later phases of surveillance; indeed as we have already noted, datasets gathered via phases 1-4 can be used in wholly unexpected ways in phase 5, algorithmic profiling. Workplaces may now conceivably use a mix of (say) manual supervision, smart tagged work lanyards or badges, e-mail and web traffic interception, tracking of work laptops and smartphones used at home, algorithmic assessment and social media scrutiny to produce an all-encompassing Panopticon.

An interesting phenomenon here is "function creep" – used here to mean the use of technologies for purposes for which they were not originally designed or envisaged by employers.[28] For example, CCTV may once have been installed in a workplace simply to establish the presence of employers, and perhaps to reduce criminal activity such as pilfering, or to discourage non-productive employees from slacking; however now in Surveillance 5.0, facial and emotion recognition techniques applied to video footage might be used to establish characteristics such as enthusiasm or commitment.[29] CCTV or video surveillance is particularly prone to such repurposing or "added value" processing; in recent months, the use of face recognition in workplaces has become particularly controversial,[30]and emotional or "affective" computing, is probably the next scandal waiting to happen. Repurposing of technological surveillance may thus increase the already heavy incursion into the private lives of employees and may be unpredictable – did employees expect standard video recording to reveal our conversations? No[31]- and hence this becomes harder to guard against.

The case study

This paper was inspired by a fortuitous "natural experiment" which offers an opportunity to study scope creep in relation to video capture, and its transformation into employee surveillance technology. In the spring of 2018, academics at 66 UK universities, who were part of the union UCU (University and College Union), embarked on strike action in response

(2017). Fair, transparent, and accountable algorithmic decision-making processes. *Philosophy & Technology*; Kirkpatrick, K. (2016). Battling algorithmic bias: How do we ensure algorithms treat us fairly? *Communications of the ACM*, 59(10), pp16-17.

[28] See also science fiction writer William Gibson's famous aphorism: "the street finds its uses for things".

[29] See McStay, A. 'Emotional AI: The Rise of Empathic Media' (Sage, 2018).

[30] See outcry at Amazon's use of a facial recognition system known as Rekognition: eg "Amazon face recognition falsely matches 28 lawmakers with mugshots, ACLU says", Guardian, 26 July 2018 at https://www.theguardian.com/technology/2018/jul/26/amazon-facial-rekognition-congress-mugshots-aclu ; and Microsoft's unusually strong call for regulation of face recognition at https://blogs.microsoft.com/on-the-issues/2018/07/13/facial-recognition-technology-the-need-for-public-regulation-and-corporate-responsibility/, 13 July 2018.

[31] See discussion of how machine learning algorithms can now reconstruct conversations from video recordings at a distance , supra n 22.

to an attempt to protest cuts in pension rights by management.[32] The strike action created a highly combative environment, and one of the outcomes was that some universities threatened to "break" the strike by replacing, without new permission or consent, striking academics with recordings of their lectures made in previous years. These recordings had been made usually for laudable, but very different, motivations such as widening access to off campus or disabled students and allowing students access to recordings to revise classes. Such systems of "lecture capture" have become widespread in the UK, but practice surrounding them eg whether recording is voluntary or mandatory and what release or permission is obtained from lecturers is, as we will discuss below, highly disparate. These threats were widely circulated on social media and created some alarm. One reason for this was that some universities had already indicated prior to the strike, either via express policies or via practice or statements, that they did use or might consider using recorded lectures to assess the performance of lecturers as well as use them as a resource for students.[33] Effectively this constitutes a type of surveillance, possibly also without notice to the lecturers concerned of the intended purpose (which might be seen as covert surveillance – see below) and possibly without an opportunity to opt out. Such surveillance could also be seen as impinging on the ability to do their job to the best of their ability; a lecture given to inform students and awaken debate, is not the same as one given expecting a score or a demerit. Our hypothesis is that the combative environment of the strike thus provided a textbook example of how an innocent and indeed socially positive data collection practice could be abused. An obvious fear would be that having seen the potential for re-use of lecture capture, the performance surveillance model might become more widespread, and become routine supplementary material in eg appraisals or disciplinary proceedings. (It should be noted perhaps that "student satisfaction" with lecturers in the UK is an important factor which is assessed by questionnaires, figured into league tables and affects the state funding a university, and individual departments within it, receive. "Excellence in teaching" as a metric has furthermore been reinforced as a funding and league table issue in England by the Teaching Excellence Framework or TEF. Put perhaps a little provocatively, surveillance of teaching quality in England and Wales can be seen as akin to CCTV surveillance of workplaces like Amazon to ensure productivity, something which has generally been seen as

[32] See https://www.ucu.org.uk/strikeforuss .

[33] See eg the St Andrews lecture capture policy https://www.st-andrews.ac.uk/media/proctor/documents/lecture-capture-policy.pdf which states that "3.9 Recordings will not be used to monitor staff performance other than in the circumstances covered by 3.11" and "3.11 the University reserves the right to consult recordings in formal disciplinary and complaint proceedings".

antithetical to an academic environment where lecturers have historically been seen as having some degree of collegiate organisation and autonomy as part of academic freedom and professional respect, rather than working under strict managerial control.

A key question is how the knowledge of surveillance might affect academic freedom. What effect does surveillance have on the ability of lecturers to teach freely and to lead students into controversial and perhaps challenging debates? There is already evidence that the knowledge of *state* surveillance can exert a "chilling effect" over writers and artists.[34] The authors, who were either union members and supporters of the strike, or affected by the strike (Martin) took the view that it was important to investigate if the law allowed this reuse of recorded lectures without consent for purposes such as not only strike breaking but also performance assessment. We undertook an informal survey in an attempt to gather information about lecture capture from the 61 higher education institutions involved in the UCU strike (the "policy survey", available online,[35] redacted in some cases to protect anonymity). Data were gathered firstly by searching individual institutions' web sites for a lecture capture policy, and additional data were gathered through a web-based survey and advertisements on social media. Although the survey did not aim to be methodologically robust it obtained a result for a large majority of institutions, even though this was sometimes a null result – ie no policy or data available. We found that of these 61 institutions, 40 had a lecture capture system ie they recorded audio or video of lectures and made them accessible to students. Policies relating to such systems were found for 28 institutions. 15 of those policies were "opt-out" – ie, a lecturer would have to make a positive choice not to be recorded. Policies varied a great deal, both in specificity and in content: the two major legal domains identified as relevant were copyright and data protection. We draw on these findings below.

The survey results along with legal advice were aired at a well-attended interactive session organised at BILETA, the UK's largest national IT law conference, in Aberdeen in April 2018.[36] As outcomes, Henderson and Edwards, alongside Prof Abbe Brown, Head of Department at Aberdeen Law School and the chair of the conference, were tasked to assist Andrew Cormack of JISC in updating the existing JISC guidance to academic institutions on lecture capture. The revised version went live on 19 June 2018 and was reportedly the most

[34] See PENAmerica survey *Chilling Effects: NSA Surveillance Drives U.S. Writers to Self-Censor* (2013) at https://pen.org/sites/default/files/Chilling%20Effects_PEN%20American.pdf which found that 1 in 6 US writers surveyed had self-censored in terms of speaking or writing about topics they thought be under surveillance.
[35] Henderson, T (2018), Lecture capture survey. Figshare dataset https://doi.org/10.6084/m9.figshare.6973847
[36] See http://bileta.ac.uk/News/&action=fullnews&id=32 .

clicked on page on the JISC site in early July.[37] BILETA guidance relating to lecture capture is also in the process of being drafted.

Regulation

General themes

As recently as 1999, Craig reviewed the issue of employee privacy and the legality of human resource policies (many of which mandated surveillance) and concluded that there was "no identifiable law of workplace privacy in the United Kingdom".[38] However, a seismic change in the legal landscape was about to happen that would "make it possible for a comprehensive body of workplace privacy law to emerge."[39] The European Data Protection Directive (DPD) 1995[40] (and the domestic Data Protection Act (DPA) 1998[41]), the incorporation of the ECHR into domestic law[42] and new domestic legislation on the interception of communications[43] were all identified as having potential to give rise a right to privacy at work. Some work on these regimes and their effects on employee privacy has been undertaken,[44] but employee surveillance remains the Cinderella sister of surveillance studies: neither as outright shocking to citizens as state surveillance in the pose Snowden era, nor as ubiquitously discussed as consumer targeting and profiling in the "surveillance capitalism"[45] ecology of social media, search and e-commerce platforms like Google, Facebook, Amazon et al.

Legal regulation has since struggled to keep pace with significant technological developments delineating the nature of scope of surveillance at work. Each time that one area has seemed to become to some extent regulated – interception of worker calls and e-mails, CCTV capture of employees - another has emerged as an unclear and only fuzzily regulated invasion of workplace privacy – "smart" surveillance, algorithmic profiling. Policymakers and courts have attempted to respond to these new challenges but as noted before, tend to lag

[37] See https://www.jisc.ac.uk/guides/recording-lectures-legal-considerations ; and private e-mail from Andrew Cormack, 30 July 2018.
[38] Craig, J. *'Privacy & Employment Law'* (Oxford: Hart Publishing, 1999)
[39] *ibid.*, p4. See also Jeffrey, M. *'Information Technology and Workers' Privacy: The English Law'* (2002) Comparative Labour Law and Policy Journal, 32, pp301-350
[40] 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.
[41] The Data Protection Act 1998 Chpt 29.
[42] In the form of the Human Rights Act 1998 Chpt 42.
[43] The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000, No.2699 (made under the Regulation of Investigatory Powers Act 2000 (RIPA).
[44] See inter alia n5, n37 and Jeffrey, M. 'Information Technology and Workers' Privacy: The English Law' (2002) Comparative Labour Law and Policy Journal, 32, pp301-350
[45] Zuboff, S. (2015). Big other: surveillance capitalism and the prospects of an information civilization. Journal of Information Technology, 30(1), pp75-89

behind technological development. A series of recent ECtHR cases have however attempted to create some principled responses to the issue of surveillance at work although even these are less fully and systematically argued than might have been hoped. This section grounds the enquiry into the regulation of lecture capture by introducing the laws currently regulating employee surveillance and then applying them to the case study.

Data Protection

The General Data Protection Regulation 2016 (GDPR)[46] replaces the existing regime building upon the existing 20 years of data protection legislation and case law. The UK has implemented the GDPR in the form of the Data Protection Act 2018 (DPA 2018).[47] Data protection (DP) law has undergone significant reformation with the GDPR modernising rules and standards for the modern digital economy, and introducing new provisions with potential to rein in employee surveillance. Further reform is also imminent with the rules on privacy in electronic communications under review.[48]The GDPR is billed as affording data subjects greater control through the strengthened threshold condition of consent.[49] Workplace surveillance inevitably involves collection and processing of personal data and historically consent has often been obtained to it as part of the employment contract or as a separate permission. Yet since the GDPR*, prima facie* consent to data processing in the employment context appears to be unattainable given the significant imbalances in power which are of the essence of the employment relation.[50] The GDPR introduces explicit provisions suggesting that consent will be invalid in the employment context as not "freely given".[51] As consent can no longer legitimise data processing in an employee surveillance situation, other threshold conditions may require scrutiny, in particular that processing is necessary for the performance of a contract[52] or that it is necessary for the purposes of the legitimate interests of the employer.[53] Furthermore, Article 88 GDPR introduces novel provisions allowing member

[46] Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.
[47] The Data Protection Act 2018 Chpt 12.
[48] See Proposal for a Regulation of the European Parliament and of the Council concerning the respect for private life and protection of personal data in electronic communications and repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications) COM(2017) 10 final
[49] Consent is defined under Article 4(11) and Article 7 GDPR. It is one, though not the only, grounds for lawful processing of personal data under Article 6 GDPR.
[50]
[51] Recital 43 and Article 7 GDPR. Pre-GDPR the A29WP strongly suggested that consent in the employment context would not be valid. See A29WP, *Opinion 8/2001 on the processing of personal data in the employment context,* WP48 and A29WP, *Working Document 2002 on the surveillance of electronic communications at work,* WP55.
[52] Art 6(1)(b) GDPR.
[53] Unless these interests are overridden by the interests or fundamental rights or freedoms of the data subject. Art 6(1)(f) GDPR.

states to enact "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".[54] Member states can introduce specific measures to safeguard the employee's "human dignity, legitimate interests and fundamental right, with particular regard to…monitoring systems at the workplace".[55]

Interception of communications

The UK has recently reformed their laws on interception of communications[56] and this has led to reissuing of the laws on workplace surveillance methods such as monitoring employee calls, e-mails and website visits. The Investigatory Powers (Interception by Businesses Etc. for Monitoring and Record-Keeping Purposes) Regulations 2018,[57] otherwise known as the Lawful Business Regulations, now permit the interception of employee communications. The previous Lawful Business Regulations enacted under RIPA2000 had been regarded as highly permissive,[58] and the new rules do not seem any narrower. Notably, it is still possible for an employer to lawfully intercept the communications (e-mails, calls, web traffic) of employees while using a system provided by work predominantly for work purposes for a wide range of reasons including "in order to establish the existence of facts", without obtaining consent, although notice is required and a record of the interception must be kept.[59]

Privacy as a human right

Since 1992 there has been human rights scrutiny of worker surveillance in the Strasbourg Court. Article 8 ECHR reads as follows:

> "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 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,

[54] Art 88(1) GDPR.
[55] Art 88(2) GDPR. So far the only EU state to take advantage of this provision has been Germany.
[56] Workplace interception of communications was previously regulated by statutory instrument (SI) made under RIPA 2000. With the replacement of that Act by the Investigatory Powers Act 2016 it was also necessary to re enact the subsidiary legislation enabling workplace interception (see n52 infra),
[57] The Investigatory Powers (Interception by Businesses Etc. for Monitoring and Record-Keeping Purposes) Regulations 2018 No.356
[58] See supra n 42
[59] Supra n 56, r 3(2)(a), r 4(1)(a) (b) and (c). Other grounds are also listed in r 3 but the breadth of r 3(2)(a) seems to render them nugatory.

or for the protection of the rights and freedoms of others."

The binary structure and qualified nature of Article 8 allows for a balance to be struck between workers' fundamental right to privacy[60] with the legitimate interests of employers (private and public sector – see below) in surveillance at work. First, the ECHR will consider whether Article 8 is engaged in the particular circumstances of surveillance. Over the years, the Courts have determined that a wide array of surveillance technologies fall within the overlapping yet autonomous domains compromising Article 8(1).[61] Significant reliance is placed upon employees' 'reasonable expectations' of privacy in determining whether Article 8 is infringed, creating the possibility of privacy protection being dependent upon employment status or the nature of work (permanent, contractor, casual labour?).As the fundamental right to privacy is not an absolute right, the Courts will then consider if the alleged interference by the state is justified under the conditions of Article 8(2). Public sector employees may complain that their employer as an organ of the state has directly interfered with their Article 8 right.[62] The state is also required to take steps to prevent citizens experiencing breaches of Article 8 in private relations (positive obligations).[63] Thus, private sector employees may claim that the state has failed to adequately safeguard or provide a legal remedy for invasion of privacy by their employer .[64] It is crucial that the binary structure of Article 8 is respected so that employees' right to privacy is not unduly restricted by competing interests and that the onus is placed on states to justify interference, accounting for their action or inaction.[65] In 1992 the ECtHR in *Niemietz v Germany*[66] clearly established the prima facie right to privacy at work stating that: *"There appears...to be no reason of principle why this understanding of the notion of private life should be taken to exclude activities of a professional or business nature since it is, after all, in the course of their working lives that the majority of people have a significant, if not the greatest opportunity of developing relationships with the outside world".*[67] Through Article 8 jurisprudence the

[60] The terms 'privacy' and 'private life' are not interchangeable. For the difference see González Fuster, G. 'The Emergence of Personal Data Protection as a Fundamental Right of the EU'(Cham: Springer, 2014), p82-84
[61] These are 'private life', 'family life', 'home', and 'correspondence'.
[62] This would constitute a breach of negative obligations.
[63] There are different ways of ensuring respect for privacy and the nature of the State's positive obligations will depend on the aspect of private life at stake. See *Söderman v. Sweden* [2013] ECHR no. 5786/08, at 79.
[64] Contracting States may fail in positive obligations by failing to adopt legislative measures or to conduct effective investigations into violations of fundamental rights.
[65] Leijten, I. 'Defining the Scope of Economic and Social Guarantees in Case Law of the ECHR' in *Shaping Rights in the ECHR: The Role of the European Court of Human Rights in Determining the Scope of Human Rights*, Brems, E. & Gerards, J. (Cambridge; Cambridge University Press, 2013) p109-136.
[66] Supra n 3.
[67] *ibid.,* at 29

Courts have incrementally addressed the privacy implications of workplace surveillance technologies.[68] The ECtHR note that the Convention is a 'living instrument' and "must be interpreted in light of present-day conditions".[69] Article 8 is not afforded an exhaustive definition and is fully adaptable to changing conditions of modern day society, thus being capable of addressing challenges brought by new technologies and changing social relationships.[70] Recently significant Article 8 scrutiny of digital era employee surveillance has taken place bringing into question the ability of Article 8 to regulate and uphold employee privacy in modern day working environments. In particular, a recent decision concerning the legality of video recording of university auditoria has provided ammunition to dispute the use of lecture capture technology (especially for the purposes of strike breaking) in UK universities.[71]

Our case study: Is use of recorded lectures for a new purpose against the will of employees legitimate?

Data protection (DP) law

In the UK, the use of video surveillance in general, not just in the workplace, has often not required the consent of those surveilled. Under the DPD, matters related to law enforcement were excluded from the general ambit of data protection law, and as a result also in the UK implementation of these laws in the DPA 1998. Where CCTV was used to detect or prevent the commission of crime, as was often asserted, there was no need to provide a lawful ground for processing of that data, such as consent.[72] CCTV became used extensively by private shops, businesses and domestic users to safeguard and record activity around their premises, without seeking permission, and this was lawful if the criminal purposes claim was made, with only notice required. Furthermore domestic householders using CCTV to surveille their own property were also exempted from the DP regime by the household or domestic purposes exemption.[73] There was no specific regulator for CCTV operations in the UK, whether for

[68] See *inter alia Halford v The United Kingdom* [1997] ECHR 32, *Copland v The United Kingdom* [2007] ECHR 253, *Antović and Mirković v Montenegro* {2017] ECHR 1068, *Barbulescu v Romania* [2017] ECHR 742. ibid.
[69] *Tyrer v The United Kingdom* [1978] ECHR 2

[70] CoE, 'Protecting the right to respect for private and family life under the ECHR' (2012), Human Rights Handbook, p9.

[71] *Antović & Mirković v Montenegro* [2017] ECHR 365
[72] See DPA 1998, s 29(1)(a) and the first data protection principle in DPA 1998, s 4 and Sched 1, Part 1 and Sched 2.
[73] DPA 1998, s 36; see now GDPR, art 2(2)(d). See on the scope of the domestic purposes exemption in relation to CCTV, the CJEU case of *Rynes v Urad,* Case C−212/13, 11 December 2014.

private or public operators, and no specific licensing regime, and indeed, it was perhaps for this very reason that the UK has become renowned as a CCTV surveillance hotspot.[74] However the other data protection principles still applied to data captured using CCTV, and supervision was increasingly applied regarding these requirements as part of the role of the Information Commissioner who issued guidance both on CCTV[75] and on employee surveillance[76] which intersected with the former. This regime is substantially re-implemented by the GDPR and the DPA 2018 although it seems that the new DP Policing Directive[77] as implemented in Pt3 of DPA2018 applies only to "competent" (ie public) "authorities" and not to private householders or workplaces[78]. This leaves private domestic use of CCTV - and use by workplaces to detect or prevent crime - in the odd position of being exempted from the GDPR but not covered by the framework of the Policing Directive. CCTV is now specifically regulated in England and Wales by a Surveillance Camera Commissioner which operates a Surveillance Cameras Code of Practice[79] but this Code and oversight only applies to public places, not workplaces.[80]

In the workplace therefore, CCTV surveillance could frequently be justified by a claim that it was there to prevent or detect crime, with only notice to employers needed. This need for notice, combined with the accumulating influence of the ECHR Article 8 case law (see above) and its influence on employment appeal tribunals, led to a general good practice assumption that a policy regarding employee surveillance and monitoring was required. This practice was reinforced by the Lawful Business Regulations which, as noted above, essentially also made employer interception of employee calls and e-mails lawful so long as clear notice was given; and by the guidance offered by the ICO which strengthened the idea that CCTV was legal if implemented with regard for the reasonable expectations of privacy of employees (see below) and with use of an acceptable use or monitoring policy of some

[74] See the famous claim from 2004 that the average Briton was caught on camera 300 times a day. https://www.independent.co.uk/news/uk/this-britain/how-average-briton-is-caught-on-camera-300-times-a-day-5354728.html .
[75] See now ICO *In the picture: A data protection code of practice for surveillance cameras and personal information* v 1.2 as of 2017 at https://ico.org.uk/media/1542/cctv-code-of-practice.pdf .
[76] See now ICO *The Employment Practices Code* at https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf .
[77] Directive 2016/680 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 of the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA.
[78] Ibid, art 2(1) and 3(7). See also DPA 2018, part III.
[79] See https://www.gov.uk/government/publications/surveillance-camera-code-of-practice, June 2013. The SCC was installed by the authority of s 30 (1) (a) of the Protection of Freedoms Act 2012. Scotland has its own scheme:
[80] See Surveillance Camera Code of Practice, supra, 1.1 and 1.9.

kind.[81]

Our case study is not, however, about detection or prevention of crime. Nor does it relate solely to domestic processing. Assuming this was admitted, university employers might turn to a number of other grounds for lawful processing given that lecture capture clearly does involve processing of personal data[82] and thus falls within the scope of the DP regime (see the very wide definition in Article 4(2) which includes *inter alia* collection, recording, consultation and use of data). Personal data captured includes the voice and image of the presenter which might also indicate qualities of, *inter alia*, racial or ethnic origin – a category of special category data (Article 9).[83] Less obviously, the content of the lecture, if it "relates to" the speaker and makes them identified or identifiable (Article 4(1)) is also almost certainly regarded as personal data, and might again be special category if it relates to one of the categories listed in Article 9. In *Nowak,*[84] the CJEU held that text written by an anonymous candidate in an exam was personal data "relating to" the candidate. It seems likely the same arguments would apply to lecture videos, and such videos, unlike exam answers, are almost impossible to anonymise because of the nature of video recording and lecture use.[85]

So is the processing involved in lecture capture lawful (Article 6, GDPR)? If a university is not seen as a public body – which is a conflicted question nowadays, at least in the UK [86] – the ground of legitimate interests (Article 6(1)(f) might be available. If it was, then the ground that the processing was carried out for the performance of a task in the public interest (Article 6(1)(e)) might be appropriate. It could also be argued that lecture capture was necessary for performance of the employment contract the lecturer had signed (Article 6(1)(b)). In both these last two cases, the use of the word "necessary", which is in post GDPR practice becoming a steadily more stringent requirement, makes the ground questionable: the

[81] See ICO supra n 75 at 3.3.2; note also *Smith v Trafford Housing Trust* [2013] IRLR 86.
[82] We refer here only to the personal data of the employee. Lecture capture may of course involve processing of personal data of the students involved. This is however outwith this paper.
[83] Although note GDPR, recital 51 which appears to indicate that racial indications drawn from video or pictorial material may not be treated as special category data unless processed intentionally to uniquely identify someone (ie as biometric data).
[84] *Nowak v DPC*, CJEU, C:2017:994, 20 December 2017.
[85] Presumably the face of the lecturer could be blurred and the voice distorted by available technologies. However this seems highly unlikely to be done and in any case the lecturer could probably be identified in most university departments by reference to timetables, websites, e-mail contact addresses etc. Note also that in *Nowak* even though the candidate's name was anonymised to the marker, the court held the data was still personal because it could be easily reidentified by the exam authorities.
[86] See disparities in legislation in the UK relating to the status of universities for tax, FOI, as a "competent authority" for DP law etc. Public authorities are not allowed to make use of the legitimate interests ground – GDPR, art 6(f).

video capture might be regarded simply as desirable not essential to the job. Much might depend perhaps on the nature of the institution, its business model or charter, and the course or programme where lecture capture took place (a distance learning programme would obviously be very different from one habitually taught in small face to face groups. A large class, where recourse to captured lectures to replace access to live teaching was commonplace but not essential might fall in the middle.) Finally of course, video capture might be legitimised by consent (Article 6(1)(a))

In practice it has probably been regarded as normal to seek consent for lecture capture and this might be done by acceptance of an overall policy or perhaps by a release signed separately at the start of the course or each lecture. It was expected by the authors that consent of some kind would be a norm because of awareness that copyright permissions would also need to be taken and recorded,[87] something universities should be very aware of, not just because of the rights of the lecturer themselves but because of the possibility of legal risk if eg copyright materials by third parties were incorporated into lectures and used/distributed to students via videos. However as noted above, collection of consent for DP purposes is not at all necessary given other lawful grounds, and in fact the newly updated JISC guidelines on lecture capture[88] still do not require or even state a preference for explicit (or even non explicit) consent to recordings in relation to data protection issues. In our policy survey, as noted above, only 28 out of 40 universities implementing lecture capture had policies. It is harder of course to know how many institutions sought discrete permissions or releases for classes or individual lectures, and no survey respondents reported this occurring. However a number of general points can be made.

First from the policy survey, a large minority of universities (15 out of the 40 using lecture capture) impose lecture capture as "opt out" ie consent presumed unless objection made. This standard of consent may be doubted as adequate, especially given the model of the newly reformed GDPR where consent must be "freely given , specific, informed and unambiguous" (Article 4(11)) and signified by a clear affirmative act and not merely by passive lack of resistance as with pre-ticked boxes or in the employment case, non-negotiable clauses.[89] Furthermore, in the GDPR, consent must be "freely given" and again, it now seems clear in the employment domain, given the inherent power imbalance, that consent can no longer act

[87] It is not possible in this paper to address copyright as well as privacy issues – a copyright release might not be necessary in an employment scenario but the issue is complex - but see the JISC guidelines as updated 19 June 2018, supra n36 for a good summary.
[88] Supra n 36.
[89] GDPR, art 4(11) and recital 32.

as a lawful basis to legitimise the processing of employee data.[90] Thirdly, in our case study we posit that videos made as part of lecture capture schemes might then be repurposed for strike-breaking or employee surveillance as performance assessment. In such a case in DP law the consent would not do to justify the new purpose of processing unless this was made clear and a new consent sought; or another ground of lawful processing used to justify the new processing. A blanket consent to unnamed purposes – such as a general release which might have been expected to cover copyright and anything else - would be insufficiently specific (Article 4(11)). A consent to "educational use" might be more dubious. We would argue that it could not be reasonably expected that educational use would include use to replace lecturers while they were on strike and as a restriction on a fundamental right, the use of consent should be interpreted narrowly.

Even if an adequate consent is obtained, or one of the other Article 6 grounds made out, a problem may arise if the lecture contains *special category* data. The grounds for lawful processing in Article 9 are much more limited than in Article 6 and in practice, the only applicable ground may be explicit consent (Article 9(2)(a)). This led one of the authors to recommend informally that to take control over use (or re-use) of lectures captured, the speaker should periodically include items of special category data in the lecture, eg, their trade union membership or religious or political or sexual opinions. This may not be a practical suggestion in every case however, and lecture footage can of course be edited (although this might itself raise issues concerning copyright, if retained by the lecturer, and the moral right to integrity).

In general therefore, it might be concluded that DP is not likely to render lecture capture, even without consent, unlawful in principle at least in the ordinary conditions of educational use. Repurposing of lecture capture footage for strike breaking (or performance surveillance) without any new consent being sought, might however well be unlawful, if based on an original consent to recording for educational purposes (say), or on one of the Article 6 non-consent grounds. Anecdotally, a number of universities do seem to have assumed they could rely on existing consents during the lecturers' strike. Much might depend on the exact nature of the wording, remembering that the GDPR firmly requires consent to be "specific" and "informed". The lack of an explicit policy or an explicit new consent might be fatal to both of these.

As indicated above, in any case DP is not the end of the story here. The ECtHR has also had a

[90] Ibid and see also recital 43 and A29WP documents cited at n 50 supra.

decisive role in ascertaining if workplace surveillance is legal with regard to Article 8 of the ECHR. Two questions are raised here: first, is Article 8 engaged – that is, is there a breach of the right to respect for private life? Second, are there reasons justifying this incursion under Article 8(2)?

ECHR: Engagement with Article 8(1)

On the first point, an amalgamation of factors affect the court's determination as to whether employee privacy has been breached under Article 8(1) including i*nter alia* the nature of the monitoring technology, the nature of activity under surveillance, and the recording, storing, processing and use of data obtained are considered. In the case of video surveillance the situation may vary depending on whether or not a policy gave adequate notice to employees of the nature and purposes of video surveillance; and whether there was or was not consent to video surveillance. A key formulation which has emerged is the reasonable expectations of the employee.

Notice and policies

In the early cases of *Halford v UK*[91] and *Copland v UK*[92] lack of notice of surveillance was a key factor in the Courts' determinations that employees' reasonable expectations of privacy at work had been infringed. These cases were driving forces in the general move towards policies around surveillance in workplaces.

Turning to our case study, our policy survey shows that in the majority of circumstances pertaining to the operation of lecture capture technology, workplace policies are in place and it is likely that awareness will thus influence whether privacy rights have been breached.[93]

However, only 28 out of 40 institutions involved in lecture capture had policies that could either be identified from the Internet or were supplied by staff in response to the survey. This is surprisingly low and often there seemed to be some confusion if a policy existed, whether it was finalised or still in development or reform, and perhaps which employees it covered. Even if a policy exists, the Courts have held that employees maintain a non-zero expectation of privacy despite notification of surveillance. The Grand Chamber in *Barbulescu v Romania*[94] held that despite awareness of internal regulations and monitoring policies, "an

[91] *Halford v UK [1997]* ECHR 32
[92] *Copland v The United Kingdom* [2007] ECHR 253
[93] The Court in *López & Ors v Spain(Application No 1874/13).*held that reasonable expectations of privacy are reinforced when employers fail to comply with legal obligations requiring employees to be adequately informed of surveillance. *López* at 67
[94] *Barbulescu v Romania* [2017] ECHR 754

employer's instructions cannot reduce private social life in the workplace to zero".[95]

The most relevant case to our case study is the recent decision in *Antović and Mirkovic v Montenegro,*[96] in which private life was found to be breached when university lecturers were video recorded, without giving their consent, during teaching in auditoria. The recordings were used to assess lecturer performance by their Dean, not to benefit students in any direct way. The University of Montenegro took the view they were entitled to do this under a local statute and that these lecture halls were public places and so the consent of lecturers or other justification was never even considered. University lecturers were, however, informed of the introduction and operation of video recording technology in university auditoria, Thus there was notice but not consent.

The Strasbourg court by contrast took the view that these auditoria were the workplaces of academics, where 'lecturers meet and interact with students whilst developing their personality and relations'.[97] Although notice had been given, the Chamber held that a reasonable expectation of privacy remained. However, the decision that Article 8 was engaged was on a fine margin (4 votes to 3) with the dissenting judges noting that "having been notified, their (lecturers) reasonable expectation of privacy in that context, *if any*, was very limited".[98] (Interestingly, there appears to be a disconnect with the approach taken to interception of communications at work under domestic UK law here. As noted above, the Lawful Business Regulations 2018 suggest that no expectation of privacy will remain once the employer has made "reasonable efforts to inform (of surveillance)".[99]

Consent

Consent to lecture capture policies can also affect whether Article 8 is engaged. We have already discussed consent in the DP section above.

The ECtHR is of course not required to be co-equivalent with the GDPR and the rulings of the CJEU on the definition of consent.[100] But it seems likely that the points discussed above concerning the inadequacies of consent in a workplace might also serve to negate the effect of any "consent" collected on reducing the reasonable expectations of privacy of the

[95] *Ibid* at 80
[96] Supra n 8 .
[97] *Antović* at 44
[98] *Antović* – Dissenting Opinion at 12
[99] The Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018, No. 356, s4(c)
[100] See eg the fracas over the case of *Delfi v Estonia* (2015) ECtHR 64669/09 in relation to intermediary liability, where the ECtHR diverged substantially from the rules in the EU E-Commerce Directive. However subsequent cases in the Strasbourg court did appear to try to remedy this rift.

employee. In *Barbulescu*, the employee was alleged to have provided consent to the monitoring of his communications and this lowered any expectation of privacy at work. However, the court doubted the validity of consent to surveillance, as the notification was neither sufficiently clear nor given in advance.[101] Consequently, the employee was found to have some expectations of privacy at work. In *Antovic*, it was explicitly noted that workplace video surveillance "entails the recorded and reproducible documentation of a person's conduct at his or her workplace, which the employee, being obliged under the employment contract to perform the work in that place, cannot evade".[102] This seems a clear reference to the impoverished nature of any consent given as part of an employment contract as well as, in that case, the actual absence of consent.

Finally the ECtHR has made it clear both in *Antovic* and *Kopke*[103] that *covert* video surveillance is "a considerable intrusion into the employee's private life". There is an interesting question to be asked here: is lecture capture imposed consensually for one purpose (widening access or lecture review) and then re-used for other purposes (strike-breaking, performance assessment) substantially equivalent to unexpected or covert surveillance?[104] Certainly although this precise scenario (repurposing) has not yet come to Strasbourg, the case law seems to indicate the court would not look favourably on this in terms of engagement of Article 8(1).

Function and nature of surveillance

Regardless of the existence of a lecture capture policy and consent to it, the employee's fundamental right to privacy may still be engaged. The nature of the activity under surveillance can also affect privacy expectations. Judge Vucini and Lemmens concurred with the majority opinion in *Antović* but believed that the Court failed to attach adequate importance to the nature of the activity that was placed under surveillance.[105] The concurring judges noted that as teaching and learning activities in universities are covered by 'academic freedom', privacy expectations of not being placed under video surveillance should be regarded as reasonable.[106]

[101] *Barbulescu* at 77
[102] *Antović* at 44
[103] *Köpke v. Germany* (dec.), no. 420/07, 5 October 2010
[104] This phrase has a technical meaning in UK surveillance law but, though used in much ECtHR case law, does not seem to have a formal definition.
[105] *Antović* – Concurring Opinions at 2
[106] *Antović* – Concurring Opinions at 4

Fascinatingly, the *Antovic* case is the inverse of the case study we present. In *Antovic,* the recordings were explicitly used for performance assessment (and allegedly to monitor and prevent thefts from lecture halls, but this was doubted by the court because the locks on the halls were sufficient for that purpose). They were not used for giving access to lectures to students. In our case study, lecture capture is almost exclusively initiated for purposes to benefit students, but is then repurposed for strike breaking or performance assessment. The first dissenting judgment in *Antovic* noted that:

> "*It seems to us that in such an interaction the teacher may have an expectation of privacy, in the sense that he or she may normally expect that what is going on in the classroom can be followed only by those who are entitled to attend the class and who actually attend it. No "unwanted attention" from others, who have nothing to do with the class. There may be exceptions, for instance when a lecture is taped for educational purposes, including for use by students who were unable to physically attend the class. However, in the applicants' case there was no such purpose*."

This seems to imply that it may not be a breach of Article 8(1) to record lectures where the purpose *is* to benefit students, even without consent. The second dissenting judgment in *Antovic* indeed took a strong line that video recording in the circumstances of the case, ie, with notice, as part of professional employment, and with limitations to the surveillance such as remote activation, reduced identifiability, access only by one person (the Dean), deletion of the recording after 30 days, and no subsequent use or re-use, was not a breach of Article 8(1) at all.[107] The dissenting judges (Judges Spano, Bianku and Kjølbro) criticised the majority reasoning, noting that the "mere fact of the amphitheatres being monitored cannot in our view engage Article 8(1) without further elements being demonstrated".[108] However it still seems likely that a *change of purpose* after such recordings are made, without consent or notice, will breach reasonable expectations, and notwithstanding the second dissenting opinion, the expectations of academic freedom of lecturers are especially significant here. The subsequent use of recorded lectures will be a crucial factor in determining whether employee privacy is infringed.[109]

Following the usual reasoning of the Courts in other employee surveillance decisions, the whole circumstances of lecture capture must thus be considered when determining if Article 8 is engaged. Differing outcomes will result, depending on whether *inter alia* audio

[107] *Antović* – Dissenting Opinion at 10
[108] *Antović* – Dissenting Opinion at 12
[109] *Antović* – See Dissenting Opinion at 10 and Concurring Opinion at 4

recordings accompany video surveillance, the quality of the lecture capture technology, any attempts at blurring or redaction, and the duration of storage and accessibility of recordings. Thus, universities have scope to distinguish their use of lecture capture technology from circumstances which are considered infringing. Nevertheless, the subsequent use of recorded lectures for purposes not originally intended or envisaged – such as strike breaking - is likely to be sufficient to infringe employees' Article 8 rights.

ECHR: Is the interference legal under Article 8(2)?

Assuming that the operation of lecture capture technology in the workplace engages Article 8, the Court will consider whether the alleged interference is legally justified under the conditions of Article 8(2). The Court will determine whether the interference is "in accordance with law", falls within the exhaustive list of 'legitimate purposes' under Article 8(2), and whether the interference is restricted to what is "necessary in a democratic society".

"In accordance with law"

Firstly, the interference with employee privacy must be in accordance with domestic law. The Court in *Copland* reiterates the requirement of 'in accordance with law':

> "*not only requires compliance with domestic law, but also relates to the quality of that law, requiring it to be compatible with the rule of law. In order to fulfil the requirement of foreseeability, the law must be sufficiently clear in its terms to give individuals an adequate indication as to the circumstances in which and the conditions on which the authorities are empowered to resort to any such measures".*[110]

The first hurdle of legality will be overcome if there exists a "measure of legal protection in domestic law against arbitrary interferences by public authorities with the rights safeguarded by Article 8(1)".[111] National legislation, common law, and other 'soft law' measures can satisfy the legality requirement so long as it is sufficiently detailed, clear and precise. The law must be foreseeable and accessible, providing individuals with adequate indication of the circumstances in which surveillance at work and dissemination of recorded lectures will take place.

In *Halford* and *Copland,* the Court held that the employees' Article 8 right was violated due to lack of domestic regulatory frameworks. Furthermore, an organisational framework and

[110] *Copland* at 45 and 46
[111] *Copland* at 45

general mandate to engage in employee surveillance will not satisfy the condition of legality. In *Copland*, the ECtHR held that despite the university's statutory purpose to "do anything necessary of expedient for purposes of providing higher education or further education",[112] this broad general mandate was incompatible with the rule of law. Nowadays, surveillance at work can fulfil the condition of legality as an array of legal sources provide protection against arbitrary interference with employees' Article 8 rights. For instance, as already noted, the Lawful Business Regulations, data protection regimes, ICO codes of conduct and guidance on surveillance at work.[113] The Court would analyse whether the aforementioned legal regimes fulfil the requirements of the rule of law, in particular, whether secondary unanticipated use of recorded lectures is foreseeable.

If the interference with employee privacy fails to comply with established legal frameworks and principles, the interference will not be regarded as in accordance with law. In *Antović*, the majority held that the interference with privacy was not in accordance with law as the university had breached the local data protection statute. In particular, the purpose of video recording of lecturers for the 'surveillance of teaching' was "not provided for by law as a ground for video surveillance".[114] The use of recorded lectures in unanticipated ways (i.e for 'strike breaking') may, as we have introduced above, constitute a breach of data protection's 'purpose limitation' principle and obligations of transparency,[115] thus failing to be "in accordance with law".

"*Legitimate purpose"*

The Court will consider whether the interference with the employee privacy falls within the exhaustive and broadly construed 'legitimate purposes' outline under Article 8(2).[116] In cases concerning employee surveillance, it is usually accepted that surveillance is legitimate for several purposes but in particular to 'protect the rights and freedoms of others'. Employers' rights in protecting their property and safeguarding the rights of students are regarded as legitimate aims which may justify surveillance. In *Antović,* the video recording of amphitheatres was accepted for the purposes of 'ensuring the safety of property and protecting students rights' but not for the 'surveillance of teaching'.[117]

[112] *Copland* at 47
[113] Supra pp 15ff.
[114] *Antović* at 59
[115] For example, see *López* , supra n 92.
[116] Beatson, J. et al., '*Human Rights: Judicial Protection in the United Kingdom'* (Sweet and Maxwell: London, 2008), 162
[117] Antović at 59

"Necessary in a democratic society"

Finally, the interference with employee privacy must be no more than is "necessary in a democratic society". The Court will undertake a test of proportionality in order to determine whether the State allows for the achievement of legitimate purposes without disproportionate impact on the fundamental right to privacy. Powers allowing for surveillance of employees and subsequent use of data must not be excessive and have adequate guarantees against abuse.[118] However, States' 'margin of appreciation' in assessing the extent of necessity of interference with employee privacy is wide due to the nature of employment, the broad discretionary powers of employers inherent in contractual relations and the lack of European consensus on the issue.[119] That said, national discretion on the matter is not unlimited.[120] Interference with employee privacy must be justified by a 'pressing social need' relating to the legitimate aim identified.[121] The Court will also assess whether domestic law allowing for the interference with employee privacy is proportionate to the legitimate aim pursued. The Court will consider whether domestic authorities have struck an appropriate balance between university, students and employees rights. However, the ECtHR have held that employers have a legitimate interest in "ensuring the smooth running of the company" and that extensive weight be afforded to how the employer wishes to achieve this aim.[122] Institutions may claim that decisions to reuse recorded lectures forms part of their broad discretionary powers to ensure the smooth running of University business.

It is worth noting however that within EU jurisprudence, the EU Charter of Fundamental Rights also offers in Article 16 the "freedom to conduct a business" and this has been regarded as an influential freedom when balanced against the fundamental and legal rights of others in a number of significant CJEU Internet law cases eg *Scarlet v SABAM*[123] (Article 16 right of ISP balanced against intellectual property rights of copyright collecting society demanding filtering or pirate works) or *McFadden v Sony*[124] (Article 16 right of ISP balanced against IP rights of rights holder). However it is rare to non-existent to see breaches of privacy justified by the business model of a company under Article 16 and indeed, it has also been held in the Strasbourg court, that a fundamental freedom cannot be defined so as to

[118] *Silver* v. *United Kingdom (1983) 5 EHRR 347*
[119] *Barbulescu* at 117 -119
[120] *Silver* at 97
[121] *Leander* v. *Sweden* [1987] 9 EHRR 433 at 58.
[122] *Barbulescu* at 127.
[123] Case C-70/10 *Scarlet Extended SA v Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM),* ECLI:EU:C:2011:771.
[124] Case C-484/14, 15 September 2016.

justify breaking the law, in this case, DP law which already incorporates into its regime a balance between fundamental rights of privacy and rights such as freedom of expression, freedom to conduct a business et al.[125]

UK employment law: an alternative approach

Cases concerning employee surveillance and violation of privacy before the UK tribunals and courts are principally advanced on the basis of unfair dismissal law. Although employees might argue that Article 8 has been breached and thus dismissal unfair,[126] their complaint against the employer is usually founded upon a breach of the mutual duty of trust and confidence. Nevertheless, Article 8 has been invoked by employees in domestic courts and tribunals in attempts to exclude evidence obtained through surveillance with varying success.[127] When Article 8 is considered to be engaged, outcomes regularly turn on whether the breach is regarded as proportionate.[128] It is beyond the scope of this paper to consider whether the mutual duty of trust and confidence can be invoked to challenge the legality of lecture capture. Nevertheless, trust and confidence has become a source of privacy protection at work due to *inter alia* Strasbourg's Article 8 jurisprudence, the incorporation of the Convention into domestic law,[129] and the corresponding interpretative obligations of domestic Courts to take into account judgments, declarations and advisory opinions of the ECtHR.[130] The mutual duty of trust and confidence has developed with potential to provide a remedy to the unanticipated use of recorded lectures for the purposes of strike breaking and also actively regulate the use of lecture capture technology in the workplace.

Conclusions

In this paper we have taken a "natural accident" case study to examine what happens and how the law responds when one type of video surveillance – lecture capture – is suddenly in adverse circumstances repurpose in a way inimical to the data subject. We have also taken into account the less mainstreamed but also threatening trend towards repurposing lecture

[125] See most notably arts 6(1)(f) and art 17(3)(a) of the GDPR. The ECtHR has held that a fundamental freedom cannot be framed to justify breaking the law : see *Vukota-Bojić v. Switzerland* [2016] no. 61838/10 and *Trabajo Rueda v. Spain* [2017] no. 32600/12, also the dissenting judgment by Dedov in the employee surveillance case of *López Ribalda & Ors v Spain* [2018] (Application No. 1874/13).

[126] See *City of Swansea v Gayle* [2013] IRLR 768, *McGowan v. Scottish Water* [2005] IRLR 167, *Turner v East Midland s Trains Ltd* [2102] IRLR 107, *Crisp v Apple Retail (UK) Ltd* ET/1500258/11

[127] See *Jones v University of Warwick* [2003] EWCA Civ 151 *and Chairman and Govenors of Amwell View School v Dogherty* [2007] IRLR 198, in which surveillance of the employer by the employee was regarded as obtained in breach of privacy and thus to be excluded from the courts considerations.

[128] See *McCann v Clude College* UKEATS/0061/09/BI and the ET and EAT reasoning in *City of Swansea v Gayle* [2013] IRLR 768

[129] Human Rights Act 1998, Chpt. 42 n

[130] HRA, s2

capture systems as performance assessment of academic staff without their consent. We found that, leaving aside national labour laws for further examination, there are two main legal routes towards asserting control of lecture capture material: data protection and Article 8 privacy rights. Data protection is unlikely to offer a clear route to banning repurposing of lecture videos without consent. Consent is only one ground for lawful processing and others may be seen as more permissive. However employers may run into difficulties if special category data is used in lectures or revealed about the lecturer and which cannot be redacted.

Article 8 is also a conflicted and dubious space in relation to workplace surveillance. The recent case of *Antovic,* which itself *did* involve the use of lecture capture without consent as performance assessment, and did *not* involve a student "widening access" educational element, seems an obvious case where the privacy argument should have won hands down. Yet in fact the court only decided by a bare majority that a breach of Article 8 had occurred, in the teeth of a strong dissenting opinion. This in itself shows both the lack of European consensus on privacy rights in the workplace, themselves only acknowledged since the 90s, and the still strong feeling that the workplace is very different from other private and public spaces where individual autonomy rights are strong and the economic and business reasons to surveille do not come into opposition.

In our case study, some specific issues come into play which do not apply to all workplace scenarios. Are academics in some way special because of their alleged rights to freedom of expression, especially in their teaching? Is the relationship between lecturer and student of close and critical, perhaps even edgy, engagement, one that might suffer from mandated surveillance, especially for future assessment in a time of increasing regard for student satisfaction surveys, worries about political correctness and disciplinarian academic management styles? Might re-use or abuse, of lecture capture lead to a reluctance to engage with it in "normal" times, which would rebound on students and especially on those most vulnerable and in need of help such as students unable to physically get to campus due to illness or special needs?. We would argue yes to all of these. The trust of academics in their management in the UK was deeply wounded by the UCU strike in general, and was damaged further by the narrative, whether true, prevalent or over-hyped, that recorded lectures might be used as strike-breaking material against their will. The trust of students might also be damaged if they felt they were being fobbed off with a second rate replacement for lectures during periods of dispute; or were being asked to be complicit in strike-breaking action against their teachers, when many student organisations had expressed sympathy for the USS

strike.

Some of the policies canvassed in our survey had positive approaches to such scenarios. For instance, Cardiff University asserted that "these lectures are taped to support student learning" and stated that any other use had to be discussed and agreed to. Cardiff, Brunel, Kings College London, Liverpool, Manchester, Queen Mary London and Sheffield explicitly stated in their policies that they did not use recordings for performance management. We recommend this formulation. We also recommend that the use of recorded lectures to replace "live" lectures during industrial action should be regarded as unethical and an impermissible breach of trust. During the UCU strike it was regarded as heartening that a number of universities saw this point and retrenched from stated positions of re-use of lectures. Finally we recommend – though this may be seen as unduly radical in its restriction of business freedom – that universities should not implement lecture capture policies at all, even for wholly beneficial motives, without obtaining the specific and informed consent of the lecturers whose personal data is captured and processed.

Finally themes can be drawn from our case study which have wider significance for the world outside academe. Increasingly surveillance technologies come onto the market which may be marketed as beneficial in some way without, deliberately or not, sufficient attention being paid to potential illegal, unethical or harmful uses. A good example is "Social Mapper": a product marketed ostensibly to discover vulnerabilities in an organisation's security. In essence, Social Mapper takes as input the names and images of workers at a company and then goes out to "correlate social media profiles across a number of different sites on a large scale" ie look on the Internet, at Facebook, LinkedIn, Instagram, Twitter et al, to find where employees hang out and what they say and do. As the Register put it:

> "In other words: even though your LinkedIn, Twitter, Facebook, Google+ (because we've all got one of those), Instagram, Russian VK, and Chinese Weibo profiles are all under different names and handles, Social Mapper can link all those profiles to you by matching a photo of your face to the selfies you used on each of the account pages."[131]

This product is marketed as a legitimate security service because these employees discoverable on social media can then be seen as weak links in the overall infosec of the company, susceptible to social engineering – a kind of "penetration testing". But it also seems

[131] See "Need a facial recognition auto-doxxx tool? Social Mapper has you covered", *Register*, 10 August 2018 at https://www.theregister.co.uk/2018/08/10/spiderlabs_social_mapper/ .

plain that this may also enable covert and ubiquitous employee surveillance, at work and outside. Should such repurposed tools be legal? Are they? If so, are they ethical? With such technologies flooding the markets, not just for employees but also for parents tracking children, disgruntled ex-partners, and others, we hope our case study may indicate some of the legal dimensions of repurposed surveillance, with a view to kickstarting a debate which should then move beyond law perhaps to commercial and professional ethics as well as to privacy by design.[132]

Another recent phenomenon we have observed has been the rise of technology-aided "wellness" programmes in offices – where employers offer, demand or link to benefits, a variety of screenings for eg fitness, weight loss, or chronic disease. Some of these involve IoT surveillance ; eg FitBits to measure and encourage employee "wellness". Gilroy-Scott, a lawyer in this area, estimates that "around 202 million wearable devices were given out by employers in 2016" as part of corporate wellness programmes" and warns that although employees and employers are both often positive about such schemes – the latter especially seeing it as a way to cut absenteeism costs – they also involve the collection of huge amounts of evidence about "location, hours worked, rest breaks and even activity levels".[133] Lyon discusses employee use of such wearables as just one of many examples of items that contribute to the normalisation of surveillance.[134] As with our case study, workers may be keen to enable such technological surveillance initially but should be prepared for when it is repurposed to achieve less expected and less desirable goals such as demotion and replacement.[135]

The road to surveillance may be paved with good intentions – but it may still be taking us somewhere that as a society we really don't want to go.

[132] There is a growing field of work around the idea of Responsible Research and Innovation (RRI) where innovators are asked to consider the possible ethical pitfalls or creating or putting into circulation their new technologies- it is beyond the scope of this paper to canvass these but we would like to include it in further work, as well as considering "privacy by design" in the creation of legitimate surveillance tools (see GDPR art 25).

[133] Gilroy-Scott, C. "Wearable fitness trackers in the workplace: surveillance by fitbit?, Personnel Today, 26 April 2017 at https://www.personneltoday.com/hr/wearable-fitness-trackers-workplace-surveillance-fitbit/

[134] Lyon, D. 'The Culture of Surveillance: Watching as a Way of Life' (Cambridge: Polity Press, 2018) ch 3

[135] Interestingly, a recent empirical study showed no causal link between such schemes and improvements in employee health or productivity or the medical spend of employers. See Carroll, A. "Why Workplace Wellness Programs Don't Work Well. Why Some Studies Show Otherwise." *New York Times*, 6 August 2018.