



LAW RESEARCH BRIEFING #7

AUGUST 2019

Employee Surveillance

The Road to Surveillance is Paved with Good Intentions



Professor Lilian Edwards

This research along with legal advice presented at BILETA (the UK's largest national IT law conference) formed the bases for updating the existing **JISC guidance to academic institutions on lecture capture**.



Research at
Newcastle Law School



Newcastle
University

This briefing presents the recent academic UCU strike action in the UK as a case study to demonstrate how technologies introduced into the workplace for beneficial reasons may morph via function creep into privacy invasive tools of surveillance.



Introduction

Employee surveillance is increasingly universal. The expansion of employee surveillance may come to undermine privacy rights in the workplace. The recent academic UCU strike action in the UK demonstrates how technologies introduced into the workplace for beneficial reasons may morph via function creep into privacy invasive tools of surveillance.

The briefing considers the negative consequences of the non-permissioned re-use of recorded lectures, which includes not just breach of trust to academics and depreciation of the employment relationship, but withdrawal from positive uses of surveillance techniques such as widening participation and enabling access.

A five-stage model of employee surveillance

Employee surveillance long precedes technological innovation. 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. This research has traced the history of employee surveillance at work through the lens of dominant technologies of each era and defined a five-phase model of surveillance development:

Surveillance 1.0 - physical and analogue surveillance;

Surveillance 2.0 - databases and dossiers;

Surveillance 3.0 - digital networked technologies;

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. 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, particularly so in the so called 'gig economy'.

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.

Lecture capture and repurposing as surveillance: the case study

In the spring of 2018, academics at 66 UK universities that were part of the union UCU (University and College Union), embarked on strike action in an attempt to protest cuts in pension rights by management. 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 usually for widening access to off campus or disabled students, and allowing students access to recordings to revise classes. Research has also demonstrated trends towards repurposing lecture capture systems as performance assessment of academic staff without their consent.



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.

Professor Lilian Edwards



Our Survey

We undertook an informal survey to gather information about lecture capture from the 61 higher education institutions involved in the UCU strike. Data were gathered by searching individual institutions' web sites for a lecture capture policy, through a web-based survey and advertisements on social media.

- Of these 61 institutions, 40 had a lecture capture systems i.e. 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" – i.e., a lecturer would have to make a positive choice not to be recorded.

Is the use of recorded lectures for a new purpose legitimate?

There are **2 main legal routes** towards asserting control of lecture capture material: **(1) data protection (GDPR) and (2) Article 8 ECtHR privacy rights.**

1. The UK has implemented the GDPR in the form of the **Data Protection Act 2018 (DPA 2018)**. The GDPR is billed as affording data subjects greater control through the strengthened threshold condition of consent. The research has showed that:

- lecture capture involves processing personal data and thus falls within the scope of the data protection regime, which includes the collection, recording, consultation and use of

data (Art 4(2));

- whether the university is seen as public or private body, Article 6 GDPR is not likely to render lecture capture, even without consent, unlawful in principle given the existence of alternate grounds such as legitimate interests.
- repurposing of lecture capture footage for strike breaking (or performance surveillance) without any new consent being sought might be unlawful,
- if *sensitive* personal data is captured e.g. race or sexuality, then explicit consent will be necessary.

2. **The ECtHR** has a decisive role in ascertaining if workplace surveillance is legal with regard to Article 8 of the ECHR. Whether employee privacy has been breached under Article 8(1) in the case of video surveillance may vary depending on whether a policy gave adequate notice to employees of the nature and purposes of video surveillance and whether there was consent to video surveillance.

The survey shows that only **28 out of 40** institutions involved in lecture capture had policies in place. Even if a policy exists, the Courts have held that employees maintain a non-zero expectation of privacy despite notification of surveillance, which needs to be clear and given

in advance (*Barbulescu v Romania* [2017] ECHR 754), while covert video surveillance is 'a considerable intrusion into the employee's private life' (*Antović and Mirković v. Montenegro* [2017] ECHR 365).

The use of recorded lectures in unanticipated ways (i.e. for 'strike breaking') may constitute a breach of the 'purpose limitation' principle in data protection law and obligations of transparency as discussed above, thus failing to meet one of the three requirements of the Court's own assessment for the violation of Article 8 (i.e. whether the interference is "in accordance with law").



Key Findings and Recommendations

- ❖ Data protection is unlikely to offer a clear route to banning repurposing of lecture videos without consent. Although, the precise scenario of this case study has not yet come to Strasbourg, the case law seems to indicate the Court would not look favourably on the repurposing of recorded (without consent) lectures.
- ❖ The trust of academics in UK was deeply wounded by the UCU strike and by the threat that recorded lectures might be used as strike-breaking material against their will. As such, the relationship between lecturer and student of close and critical engagement might suffer from mandated surveillance, especially for future assessment in a time of increasing regard for student satisfaction surveys.
- ❖ The use of recorded lectures to replace "live" lectures during industrial action should be regarded as unethical and an impermissible breach of trust. 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.

Professor Lilian Edwards



Prof. Lilian Edwards is a leading academic in the field of Internet law. She has taught information technology law, e-commerce law, privacy law and Internet law at undergraduate and postgraduate level since 1996 and has been involved with law and artificial intelligence (AI) since 1985. She is the Associate Director, and was co-founder, of the Arts and Humanities Research Council (AHRC) Centre for IP and Technology Law (now SCRIPT). She has consulted for the EU Commission, the OECD, and WIPO. Prof. Edwards is a co-investigator at Newcastle in the PETRAS Internet of Things Hub and a partner in the Horizon Digital Economy Hub at Nottingham.

 lilian.edwards@ncl.ac.uk

 [@lilianedwards](https://twitter.com/lilianedwards)

 www.ncl.ac.uk/nuls



Edwards, Lilian and Martin, Laura and Henderson, Tristan, 'Employee Surveillance: The Road to Surveillance is Paved with Good Intentions'. *Technology and Regulation* (forthcoming 2019).

Please cite this document as: Lilian Edwards, 'Employee Surveillance: The Road to Surveillance is Paved with Good Intentions' (2019) Newcastle Law School Research Briefing No 7

