



Opinion. Privacy, Personal Information and Employment.

Andrew J. Charlesworth¹

Abstract

It is a widely accepted proposition, reflected in privacy-enhancing legislation and regulations, that individuals will have less privacy in their workplace activities than in their private lives. However, modern technologies and business practices have blurred the boundary between private life and workplace, and a re-evaluation of the traditional legislative and regulatory protections for privacy in employment is required.

While the 'right to privacy' is often spoken of as if it were a commonly understood and accepted principle, over the years privacy has continued to be a difficult concept to pin down. Lawyers, philosophers and sociologists have all attempted to provide a comprehensive definition of privacy and then to explain why there should be a right to it, or alternatively, why there should not. None of the accounts has swept all before it, although some may seem more convincing than others, in that they relate more closely to our own innate concept of what privacy means. Thus Richard A. Posner's account of privacy, couched as it is in the language and logic of legal economics, may resonate with us less than Amitai Etzioni's communitarian account, although both writers suggest that the extent of an individual's right to privacy must necessarily be significantly restricted for the greater good of society.

In practice, any writer wishing to outline a general theory of the right to privacy rapidly discovers that, upon subjecting that theory to the acid test of practical experience, the right of privacy in any given situation is inevitably proven to be largely contingent upon circumstance. The degree to which a right of privacy is developed and respected, and the behaviours and activities that are affected, varies from community to community and is thus heavily dependant upon a range of societal norms. As a result, the 'right of privacy' in a medieval village differs from that of the modern city, that of the Tuareg differs from that of the Californian, that of the prisoner from that of the jailer, and that of the 'cyberspace' purchaser from that of the 'meatspace' purchaser.

In fact, in contemporary Western society, an individual's expectation of privacy will differ widely at various points in their day, according to their location and particular activity, with the degree of expected scrutiny differing between, for example, the home,

¹ Senior Research Fellow in IT & Law, Director of the Centre for IT and Law, Law School/Computer Science Department, University of Bristol, UK. <mailto:a.j.charlesworth@bristol.ac.uk>

the shopping mall, the motorway, and the workplace. Even within those areas there are often further degrees of privacy to consider - the bathroom in the home, the changing room in the shopping mall, and the lunch break in the workplace. Much of our conception of privacy remains predicated on the protection of our physical privacy although, in the Western society, invasions of both our informational and decisional privacy have increasingly assumed a greater practical importance. Thus, while the ubiquity of CCTV cameras in British cities, towns and villages may foster concerns about the invasion of our privacy, as our ability to simply be anonymous in public places - an unrecorded face in the crowd - is gradually eroded, the recording and interpretation of our informational paths may often pass largely unremarked. The fact that our home digital satellite TV box is hooked up to our telephone line to pass information about our viewing habits back to the suppliers, or that our cyberspace activities from our home computer are monitored by 'cookies', 'web bugs' and other hardware and software information-gathering devices means that our expectation of privacy in the home, premised on the prevention of physical invasion of that space by others without good cause, may no longer be squared with the reality of the informational privacy invasion of the home that has been made possible by advances in technology. The clear line between the zone of privacy within the home, and that without, is thus gradually blurring, even without consideration of the proposed use of publically contentious law enforcement technologies, such as heat sensors, to permit the monitoring of domestic activities without the need to physically enter private premises.

This blurring of the sharp lines between established zones of privacy is evident in the area of employment. We may look back with mild amusement at the social engineering activities of Victorian-period industrialists such as Titus Salt in the UK and Hiram Walker in the US, whose model communities certainly provided living conditions for the workers which were far better than those generally prevailing at the time, but were also designed to allow the factory owners to surveil and thus to influence directly or indirectly the activities of their employees outside the work place; but the degree of potential interference in the private lives of employees by employers today may be viewed as no less perturbing, particularly given the array of modern surveillance techniques available. The modern employee may be watched via CCTV whilst working in the (open-plan) office, her telephone calls recorded, her office conversation monitored by listening devices, her key strokes logged, her computer screen monitored, her movements noted by sensors in her seat, her whereabouts in the building pinpointed by location badge. She may also be obliged prior to, or during, her employment to submit to urinalysis, personality testing and genetic screening and monitoring. The former mechanisms may be seen to erode privacy in the workplace; the latter to extend to additionally threaten the employee's privacy outside the workplace.

The workplace mechanisms may be disliked by employees, but are, perhaps, more likely to be tolerated, in that the common perception of the workplace is of an environment where an individual's privacy is likely to be significantly reduced, and that this reduction is a price not unreasonably paid for the benefits of employment. The mechanisms with the potential to intrude into areas outside the workplace, into what many would term the 'private life' of the individual, are thus likely to be more controversial for, it can be

argued, what business is it of the employer what the individual does in their own time and away from the employer's premises? And what right does an employer have to know medical or genetic information about an employee, particularly when that information may only indicate a possible predisposition towards a particular medical condition?

The approach taken by the law, or by regulators, to such issues has often appeared to reflect these perceptions - that an individual has little or no expectation of privacy in the workplace, but that attempts by employers to obtain information about, or assert control over, aspects of an employee's life pertaining to life and activities outside the workplace should be subject to much greater legal scrutiny and control. More recent developments, however, may suggest that, on the surface at least, the legal and regulatory approaches to privacy in the workplace have undergone something of a sea change. Both the Regulation of Investigatory Powers Act 2000 and the Information Commissioner's Code of Practice on the Use of Personal Data in Employer/Employee Relationships suggest that tighter controls are being exerted over the monitoring of employees by employers, in particular in the requirements that certain types of monitoring be conducted for specific purposes and in an open manner, and that information so collected should be treated in accordance with the Data Protection Principles.

Both developments have, not unnaturally, been received with expressions of dismay by some employers and their lobbying groups, whilst being hailed by trade unions and other employee representatives as a step in the right direction in ensuring adequate privacy protection in the workplace. Detractors have also attacked them as further evidence of the creeping Europeanization of the British legal system, as both developments have come about largely because of pressures from the ECHR and EU. In practice, it is debatable as to whether either development will have a significant effect on employee privacy in the average workplace. The Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 provide wide provision for the legitimate monitoring and recording of workplace communications within the framework of the Regulation of Investigatory Powers Act 2000, and the Information Commissioner's Code of Practice on the Use of Personal Data in Employer/Employee Relationships whilst influential, does not itself have the force of law.

Certainly, it would seem that neither of these developments would have a significant impact on the current debate concerning the extent to which employers can monitor, or utilise information about, employee behaviour outside the workplace. For example, a key area of contention at present is the issue of smoking. Most workplaces now have strict smoking policies, with employees who smoke required to do so in special smoking areas on the employer's premises, or simply not to smoke on the premises at all - the small huddle of dedicated outdoor smokers is now a common sight in public spaces outside many modern office buildings. The question is, just how far can employers insist that their employees refrain from indulging in a nicotine habit? Can employers legitimately require their workers not to smoke even when away from the employer's premises, and outside working hours? If they can legitimately make such demands, how is employee compliance to be verified? In the US the penchant for drug testing is already widespread amongst employers, and it would be a simple matter to add nicotine and/or its breakdown

products to the lists of substances tested for. However, a number of the US states have laws making it illegal to discriminate against employees or potential employees because they smoke during nonworking hours. In the UK, such testing is, if not unusual, certainly considerably less common, and it is interesting to consider how testing for a substance which is perfectly legal to use would square with the right to respect for an individual's private and family life.

It is true that, as a smoker, an individual will be more prone to certain types of disease, and that smoking-related illness, if it occurs, will affect their performance as an employee. It may also be the case that, if denied their nicotine fix during working hours, that they may exhibit behaviours uncondusive to the efficient workplace, including loss of concentration and irritableness. Smokers are also more costly to insure. Yet are these potential costs to the employer sufficient justification for the degree of intrusion into the individual's private life required to police a strict no smoking policy. At what point does an employer's right to know about its employees' behaviour end - if an employer can legitimately inquire about smoking during non-working hours, what about drinking or participation in extreme sports?

Posner's economic approach suggests that the employer should have the right to know all relevant information about its employees both prior to, and during, their employment, for in the absence of this knowledge the employer cannot make an accurate assessment of the value it will accrue in return for the benefits that it is offering - there is a risk that the employer will hire employees whose cost in terms of salary, pension, insurance, and other benefits will be significantly higher than their return, due to poor productivity, sick leave or death. Posner questions the right of the individual in such circumstances to withhold information that may be directly relevant to the employer's ability to make that assessment. One might even go as far as to say that, in some circumstances it would be defensible to describe the withholding of such information as being tantamount to fraud upon the employer.

This type of analysis leads very rapidly, however, to difficult questions about the extent to which an employee should have to disclose factors that might impinge on that assessment, where such factors are entirely outwith the control of the employee, and may in fact be unknown to them - an example being genetic predisposition to certain types of illness. If we follow the above approach, it would appear reasonable for an employer to require employees to be tested for certain genetic traits, and to then make decisions concerning employment based on the information elicited. However, such an approach is bounded by difficulties - perhaps the most obvious of which is that genetic predisposition towards a disease is by no means the same as a certainty that an individual will eventually suffer from the disease - and such testing, while not unheard of, remains controversial. This area has, as a result, elicited considerable jurisprudential and philosophical debate. What it has not produced, however, is much in the way of useful law, either from the courts or from the legislature, in which such difficulties have been properly assessed.

In conclusion, it appears that there are common understandings about privacy in the workplace; not least that many activities in the workplace will be afforded less protection

than if they occurred in the home, for example, telephone calls and e-mails to and from the workplace. Indeed, workers may even resist 'privacy-enhancing' measures where these interfere with their ability to do their job by, for example, interfering with workplace communication. The law relating to such issues is thus, relatively speaking, uncontentious - for all the initial furore about the Regulation of Investigatory Powers Act 2000 and the Information Commissioner's Code of Practice on the Use of Personal Data in Employer/Employee Relationships, such measures in fact do little more than codify what were essentially workplace norms - personal calls from work are not the same as personal calls from home; employers will check to see that workers are in fact working; employers may hold and use personal data on employees if they do so fairly. Much of the employer discontent about the measures thus stemmed mainly from uncertainty about what they required, rather than active opposition to their practical implications. Management are, after all, highly likely to be influenced by the same normative privacy considerations as their employees, and both groups can thus relate to the distress that breaches of those considerations may cause, and comprehend when the line between acceptable and unacceptable behaviour will be perceived by others to have been crossed.

Where problems arise is in those areas where no common understandings exist, usually because they have not had time to develop and mature, and where the implications of the development of those areas contain threats for which, at present, there are no obvious social or legal safeguards. Such situations may arise when existing areas with established common understandings are subject to radical change. For example, the boundary between home life and workplace has long been part of the common understanding - metaphorically the employer's writ ceases, if not at the exit of the workplace, then certainly at the entrance to the home. However, due in part to developments in both workplace and surveillance technologies, but also to changes in the demographics of employment; as the migration from the primary and secondary industries of extraction and manufacture to the tertiary industries of services and information provision continues, that 'bright-line' boundary has become increasingly blurred. This is further exacerbated by employment practices such as the replacement of 9 to 5 working hours with flexi-time, and the increased popularity of 'telecommuting' where employees undertake some, or all, of their employment duties via electronic communications from their homes. With the blurring of that boundary, workers are likely to find employer interventions increasingly affecting their 'home space' or 'private space', and those interventions, in breaching the traditional normative privacy accorded to that space, are inevitably going to be regarded, initially at least, as unacceptably intrusive, and thus resisted. From an employer's perspective, however, such interventions may seem reasonable where accepted mechanisms for establishing a controlled workplace environment, including understood levels of workplace surveillance, have been rendered less effective by those changes in both the nature of employment and of the workplace. The original common understanding between employer and employee thus collapses.

Establishing or re-establishing a common understanding in this area, or in any other, may not be an easy task, in part because the shift in employment and working practices is ongoing. The key principles that will have to be considered by those tasked with legal and regulatory oversight of the employer/employee relationship, and indeed by

employers, employees and their respective representatives have, however, already largely been delineated in the information privacy arena. Thus, measures which are intrusive on the privacy of the employee should:

- Have a legitimate purpose - employers should identify a purpose for adopting a privacy-intrusive employment measure, and only utilise the measure in accordance with that purpose. The purpose should be set out in advance of a measure's application, and be readily demonstrable to employees.
- Be proportionate - employers should be able to demonstrate that the cost of achieving a purpose, in terms of intrusion into individual privacy, is outweighed by the gain accruing to the employer and/or society from it, and should also ensure that any measure adopted is the least privacy-invasive procedure available to achieve that purpose.
- Be fair - when an employer has identified a particular purpose, they should also be obliged to consider its fairness and lawfulness in terms of the employer/employee relationship.
- Be applicable equally - a purpose, or the measure used to achieve it, should not unlawfully discriminate between employees.
- Be transparent - employees should be informed of the purpose of the measure, and the steps that the employer has taken to ensure that the measure is fair.