Privacy and organizational communication theory

Introduction

This essay will consider and evaluate the proposition “ privacy is dead- get over it” by looking at organizational communication theory and practice. The essay will look at the role of the employee in the modern corporate environment, and compare and contrast this with the role and status enjoyed by the employee in more historical settings. The essay will look at the statutory framework for Data Protection in the UK, and privacy and will examine how this applies to the workplace, both in theory and in practice. The role of legislation designed to protect the interests of employees will be considered and the writer will comment on the efficacy of the legislation as well as considering the specific rights that it creates for employees and the specific responsibilities that it creates for employers. The wider sociological context for issues connected to surveillance in the workplace and employment rights will be examined also, and the writer will consider how technological advancement and the Information Age has affected the status of the modern employee in terms of their privacy. The ultimate aim of creating this context will be to inform a holistic evaluation of the proposition “ privacy is dead- get over it”.

Privacy and surveillance in the workplace

In the modern workplace there are various tensions that exist between the privacy of employees and the level of surveillance that employers may employ in order to ensure that the organization functions optimally (Sprenger, P. (1999); Treacy, B. (2009); Wilkes, A. (2011)). Social networking sites are becoming more and more popular, and the internet is being used more and more to facilitate communication within organizations: “ According

to the Office for National Statistics' 2010 data, 30. 1 million adults in the UK (60% of the population) access the internet every day or almost everyday. This is nearly double the 2006 estimate of 16. 5 million. Social networking was a popular internet activity in 2010, with 43% of internet users posting messages to social networking sites or chat sites, blogs etc. While social networking activities prove to be most popular amongst 16–24 year olds, 31% of internet users aged 45–54 have used the internet to post messages on social network sites, while 28% uploaded content. Many of the adults that use social networks do so not only for social networking purposes but also for business networking purposes. Of the individuals listed in LinkedIn this year, there are over 52, 000 people, predominantly in the US, Canada, India, Italy, UK and the Netherlands (in that order) with ' privacy' mentioned in their profile. Within LinkedIn there are also a considerable number of privacy related LinkedIn groups which have substantial memberships. Many of the readers of this article will no doubt be in those groups for social as well as business purposes...(Bond, R. (2010) pp. 1)", and this intensifies the debate as to how far employees' privacy can be lawfully infringed by employers.

As organizational communication takes place more and more via email and other forms of electronic communication the problem of privacy is further heightened as more extensive records of personal communication are created and retained (Johnson, D. and Turner, C. (2003) p. 43-47; Jordan, T. (1999) p. 17-19; Kitt, G. (1996) p. 14-18). What to do with data like this poses a complex problem relating to the privacy of the employee and the right of the employer to infringe privacy in order to ensure the integrity of their organization.

The statutory framework

In the UK the privacy of an employee's data, and an employer's lawful access to such information is defined through a number of routes (Lunney, M. and Oliphant, K. (2003); Mc Kendrick, E. (2003)). Firstly, there is an important statutory framework that employers must respect. This is created by the Data Protection Act 1998, and also by the ECHR which requires that an individual's private and family life be respected (Article 8 of the ECHR). These rights are enforceable by an individual in a civil court in the UK, but also by public agencies in the UK like the Office of the Information Commissioner (Sprenger, P. (1999); Treacy, B. (2009); Wilkes, A. (2011)).

The Data Protection Act 1998 has created a number of principles of data protection, which must be respected. These are that information (i) must be fairly and lawfully processed; (ii) information may only be obtained for specified lawful purposes, (ii) may not be processed in any manner incompatible with such purposes; (iii) data must be adequate, relevant and not excessive for the purposes for which it is collected; (iv) information must be accurate and where necessary kept up to date, (v) information must not be kept longer than necessary, (vi) information must be processed in accordance with the rights of data subjects, (vii) security measures must be taken against unauthorized and unlawful processing of information against accidental destruction, or unauthorized or unlawful destruction, and (viii) information must not be transferred outside the European Economic Area within the consent of the data subject. In cases where these principles are not adhered to by employers, an employee may institute civil actions for breach of privacy, and or complaints to the ICO who may pursue criminal

prosecutions against any party who has breached the Data Protection Principles (Kuschewsky, M. (2009); Hansson, S. and Palm, E. (2005) p. 57). As such the Data Protection Act 1998 creates a range of rights in terms of privacy and security of personal information and these may be enforced directly by an individual or by a public body such as The Information Commissioner on behalf of an individual. Breach of the Data Protection Act 1998 is a criminal offence which is punishable with fines and or up to six months imprisonment. Recent changes to the powers of the Information Commissioner gives them powers to issue fines of up to £500, 000 for cases of serious breaches of the Data Protection Act 1998 (Kuschewsky, M. (2009); Hansson, S. and Palm, E. (2005) p. 57).

On the other hand there is also a statutory framework that addresses how far an employer may go in terms of monitoring their employees in the course of employment. The Regulation of Investigatory Powers Act 2000 and the Telecommunications (Lawful Business Practice) (Interception of Communication) Regulations 2000. These provide that monitoring of employee data can only be authorized for specific, defined purposes such as where the employer has a legitimate overriding interest in the pursuit of monitoring activities (Schirato, T. and Yell, S. (2000) p. 42-45; Sime, S. (2007) p. 12; Smith, M. and Kollock, P. (1998) p. 32-35). Thus it may be argued that there is a balance to be struck between the information that employee’s disclose which may be lawfully evaluated by the employer (deemed for example in communication privacy management theory as “ self-disclosed” information (see: Petronio, S. (2002) p. 3)) and information that is subject to inappropriate uses.

Clauses in the employment contract may also define the rights and responsibilities of the employer and the employee in terms of privacy, but it is important to note that employers may not, through the operation of a private contract exclude any of the rights and or responsibilities that are defined in The Data Protection Act 1998, or the ECHR (Blanpain, R. (2007); Elliott, C. and Quinn, F. (1999)). The wider legislative framework may be further defined according to the theory of privacy rule development. Privacy rule development theory argues that cultural, and sociological factors impact the boundaries of privacy rights (Petronio, S. (2002) p. 40) and it is clear that there is a balanced approach to the rights of the employee and the responsibilities of the employer under this framework and this reflects wider liberal sociological and cultural values prevalent in the UK.

Management Information Communication Systems and Monitoring Strategies

Different strategies may be adopted by organizations in terms of monitoring their employees. Historically, opportunities for monitoring were limited for example in relation to workers on shop floors or in a physical office environment (Freedman, J. (1994); Fletcher, I. (2001)). In modern times employees may be monitored in terms of the keystrokes that are used by them or their computers or at their work stations. Additionally, the use of smart cards and CCTV monitoring of employees may give employers extra information with which to monitor the activities of employees (Kuschewsky, M. (2009); Hansson, S. and Palm, E. (2005) p. 57). There is also a valuable market for the use of computer products that allow employers to monitor employees, for example Spector Pro which uses the slogan “ when you absolutely need to know everything they are doing online”. The use of

products and services such as this is referred to as the embedded approach to workplace surveillance, where the employer “ tracks” the activities of the employee mainly through the use of computer based products. Companies are undertaking proactive strategies like this to assess what is the most appropriate way to monitor employees, while striking a balance between effective monitoring and preserving staff morale, a case in point being Servisair which undertook a holistic risk assessment of the organizational monitoring practices in their company and concluded that methods of monitoring of employees needed to be improved across their organization. It is clear that in the Information Age, managers have much more information at their disposal that allows them to make more informed choices as to the vetting of possible future employees, and also the performance of current employees (Kuschewsky, M. (2009); Hansson, S. and Palm, E. (2005)). All of these changes raise attendant privacy issues.

An organizational communication perspective – is privacy dead?

The question of whether privacy is dead is a complex issue. A simple example might be that an employee viewing pornography at their work station in circumstances where they are unaware that the employer may be able to access their computer also and view their electronic “ history”, might be disciplined or dismissed by that employer. The employer who instituted disciplinary action against such an employee may be seen to have acted in a justified manner. However, there are also cases where the dividing line between the rights of privacy and the responsibility of the employer to respect that is less clear.

Several cases for example highlighted in the media recently have involved employees “ off sick” who were disciplined or dismissed when it later transpired that they had been using social networking sites during their time off, casting doubt of the veracity of their claims to illness (Moult, J. (2009)).

What to do regarding data recovered as a result of a third party data breach represents another difficult issue for employers: “ there was considerable media attention drawn to the fact that a security consultant, Ron Bowles, had used a piece of code to scan Facebook profiles collecting data not hidden by the user’s privacy settings. The scanned list of profiles was then shared as a downloadable file across the internet, and allegedly caused privacy fears for the 100 million users of Facebook whose personal data were compromised. The reaction by the media and regulators to the exposure of personal data in the new social media platforms of Facebook, Google and the like, tends to be focused on the intrusion on individuals’ privacy. When personal data are compromised in the realm of social media, the media reaction is to blame the SNS provider for, firstly, not having enough security in place and, secondly, for not having done enough to draw the attention of users to the need for them to manage their own privacy in terms of privacy settings and privacy parameters……(Bond, R. (2010) pp. 3)”.

Other cases have been highlighted where comments published by employees in reference to their employers on social networking sites have led to dismissals, and or disciplinary action where these have amounted to unauthorized disclosures of information, or unwelcome criticisms of the employer (Moult, J. (2009) and see also: Freedman, J. (1994); Fletcher, I. (2001)). In terms of the employee, it is also the case that records of email

communication can be viewed by employers on a Master server computer, and so whereas an employee may be under the impression that their personal work email may be used for personal communication, they may not be aware that an employer could also have access to these records of communication (Sprenger, P. (1999); Treacy, B. (2009); Wilkes, A. (2011)). Kuschewsky, M. (2009) highlighted a case recently where an employer was prosecuted by the ICO for compiling a database of personal data on employees to include information about their personal lives, employment history, personal relationships, political affiliations and trade union membership. The database was seized by the ICO during the course of criminal proceedings relating to the Data Protection Act 1998, and it emerged that the database had been used by up to 40 construction companies for employment vetting without the knowledge of the employees. The consultant managing the database was prosecuted by the ICO for failing to inform the employees that their personal information was being used in this way, and the ICO considered taking legal action against the construction companies for using the information inappropriately (Kuschewsky, M. (2009); Hansson, S. and Palm, E. (2005) p. 57).

Surveying all of this information about how the status of the employee has been affected by technological developments, it is easy to see why some scholars might argue that privacy is dead. The fact is that privacy is something that is a lot more difficult to preserve in a modern working environment. Social networking sites and activities on these provide a prime example of why. Whereas one hundred years ago an employee’s private communications between their friends about their work would be largely

inaccessible to an employer (Johnson, D. and Turner, C. (2003) p. 43-47; Jordan, T. (1999) p. 17-19; Kitt, G. (1996) p. 14-18), this has changed considerably as real-time electronic communications create considerable amounts of data for employers to use to evaluate the employee and their performance at work (Freedman, J. (1994); Fletcher, I. (2001)). Commercial profiteering has also grown up around the vetting of employees, as the case of the ICO prosecution of a security vetting consultant discussed above highlights. Organizations for example have emerged that compile databases of individuals that may be searched to give employees extra information about the employee, and so it is becoming more and more difficult for an employee to " hide" a gap in their work-history, a dispute with a previous employer, a dismissal or even a poor credit history due to the risk that an employer may be made aware of it as a result of their vetting process (Kuschewsky, M. (2009); Hansson, S. and Palm, E. (2005) p. 57).

In terms of the proposition it is however submitted that it must be rejected. Privacy in the workplace is not dead. If anything, the exact opposite is true in that employees have a range of rights that are specifically designed to protect their privacy in the workplace, the most notable being the prospect that the ICO would choose to pursue criminal prosecutions against an employer (Sprenger, P. (1999); Treacy, B. (2009); Wilkes, A. (2011)). In this respect it may be argued that the status of the employee subject to monitoring in their work is subject to growing protection by an ever-increasing range of rights that are being enacted by policy-makers. In this regard the influence of the EU is of particular significance, since the impetus for the enactment of the Data Protection Act 1998 in the UK lay in a 1995 EU

Directive on data protection (Kuschewsky, M. (2009); Hansson, S. and Palm, E. (2005) p. 57). An example that highlights this is the Data Protection Act 1998 and the growing powers that the ICO can apply to employers who abuse the personal information of employees. As Kuschewsky (2009, pp. 2) notes for example employees cannot be forced to submit to surveillance in the workplace in the absence of informed consent, and genuine choice as to their consent. Further employers are required to demonstrate that there is a specific need for the surveillance practice to be pursued. Thus, in a sense any surveillance practice employed by an employer is subject to another type of " surveillance", and in cases where inappropriate practices are identified employers can incur significant financial penalties which can lead to significant civil liability to employees (Kuschewsky, M. (2009); Hansson, S. and Palm, E. (2005) p. 57).

It may be argued that rather than privacy being dead, it is the case that more and more information is entering the public domain and this information may be used by employers to limit the rights of an employee. The distinction to be drawn is significant though. If privacy may be seen as something that employees enjoy less and less, this is not a function of privacy regulation, but rather a function of information and the amount of information that is available regarding employees in the workplace (Kuschewsky, M. (2009); Hansson, S. and Palm, E. (2005) p. 57). The distinction between the relationship of privacy to privacy laws and regulation and the relationship of privacy to information and its availability is important, because it is the central tenet under which the proposition " privacy is dead" may be rejected. It must be remembered that just because information may

be available, it is not the case that employers can simply do what they wish with it. As more and more information becomes available to employers, policy-makers are responding by imposing regulation as to what is an appropriate use of information, and setting out statutory powers that may be used to act against employers who have abused the trust of employees who have made their information available to them (Johnson, D. and Turner, C. (2003) p. 43-47; Jordan, T. (1999) p. 17-19; Kitt, G. (1996) p. 14-18).

Conclusion

This essay has argued that the Information age has changed the status of the employee significantly. The increased use of email and other forms of electronic communications in the workplace has meant that a modern employer typically holds a great deal more information about the employee than would have been the case one hundred or even fifty years ago. Additionally, the divide between a person's personal life and a person's status as an employee is lessening with the use of social networking sites (Kuschewsky, M. (2009); Hansson, S. and Palm, E. (2005) p. 57). There has also been a commercialisation of employee monitoring and this can lead to the adoption of information systems and products to appraise the performance of employees in terms of " tracking" their activities online, and creating statistical profiles of their internet use. The case of Servisair was discussed to highlight this, and many other corporate organizations are attempting to reduce the risks that they are exposed to in employing employees by gathering information about their personal lives, financial interests and also their activities while they are at work (Johnson, D. and Turner, C. (2003) p. 43-47; Jordan, T. (1999) p. 17-19; Kitt, G. (1996) p. 14-

18). The result is that employers have much more opportunity to review the performance of employees. It is not the case however that these changes have taken place in a vacuum. In the UK at least a strict statutory regime has grown up around issues of privacy, the most important being the Data Protection Act 1998 and the ECHR. These have created privacy rights in both the private and the public sphere (Johnson, D. and Turner, C. (2003) p. 43-47; Jordan, T. (1999) p. 17-19; Kitt, G. (1996) p. 14-18), as employers face the prospect of fines and criminal prosecutions in cases where it is found that they have abused or inappropriately used information regarding an employee (Kuschewsky, M. (2009); Hansson, S. and Palm, E. (2005) p. 57).

It has been argued therefore that as more and more information has become available to employers, employers have been fixed with more and more responsibility to use this information appropriately. The development of the legislative framework in the UK highlights this, with the development of the Data Protection Act 1998 as well as the public law agencies such as the ICO who are empowered to enforce it. A case in point was the case highlighted by Kuschewsky, M. (2009) where a security consultant hired by 40 construction companies to provide vetting services regarding construction workers was prosecuting under the Data Protection Act 1998 for breaches of the data protection principles (Kuschewsky, M. (2009); Hansson, S. and Palm, E. (2005)). It is clear therefore that whereas employers can reduce risk by carrying out dubious vetting practices, there are also many risks that corporations are exposed to in cases where they abuse personal information, or when they infringe the rights of employees to enjoy a reasonable level of privacy. The default position that is encouraged is one where an appropriate

balance is struck between the rights of the employee to privacy and the responsibility of the employer to respect privacy.

On the whole the writer has rejected the proposition that privacy is dead, because there is clear evidence that privacy is something that employers need to respect if they are to avoid criminal prosecution and the risk of litigation by disgruntled employees (Kuschewsky, M. (2009); Hansson, S. and Palm, E. (2005)). It has instead been argued that, rather than privacy being dead, privacy is just harder for employees to maintain in the Information Age. This, it has been suggested is a function of the availability of information, and not a function of the status of privacy. If anything privacy has become something that employers need to be more and more aware of, albeit in circumstances where much more information is available to them as to the performance of an employee.

References

Bond, R. (2010) Data Ownership in Social Networks – A Very Personal Thing. Privacy and Data Protection. 11 1 8 (Nov)

Blanpain, R. (2007) The Global Workplace: International and Comparative Employment Law. CUP. UK.

Elliott, C. and Quinn, F. (1999) Contract Law. Longman, UK.

Freedman, J. (1994) Small Businesses and the Corporate Form: Burden or Privilege? The Modern Law Review (Vol. 57) (4) pp. 555-584

Fletcher, I. (2001) A Small Business Perspective on Regulation in the UK. Economic Affairs. Vol. 21 (2) pp. 17

Hansson, S. and Palm, E. (2005) The Ethics of Workplace Privacy. Lang. Brussels.

Jensen, K. (2002) A Handbook of Media and Communication Research: Qualitative and Quantitative Methodologies. Routledge. UK.

Johnson, D. and Turner, C. (2003) International Business- Themes and Issues in the Modern Global Economy. Routledge. UK.

Jordan, T. (1999) Cyberpower: The Culture and Politics of Cyberspace and the Internet. Routledge. UK.

Kitt, G. (1996) Advanced Organizational Structures. Elan. UK.

Kuschewsky, M. (2009) Surveillance at the Workplace – How to Avoid the Pitfalls. Privacy and Data Protection. 9 6 (8) (June)

Lunney, M. and Oliphant, K. (2003) Tort Law. OUP. UK.

Mc Kendrick, E. (2003) Contract Law. Clarendon. UK.

Moult, J. (2009) Woman Sacked on Facebook for Complaining About Her Boss after Forgetting She Had Added Him As A Friend. Available at: http://www. dailymail. co. uk/news/article-1206491/Woman-sacked-Facebook-boss-insult-forgetting-added-friend. html

Petronio, S. (2002) Boundaries of Privacy: Dialectics of Disclosure. SUNY. USA.

Schirato, T. and Yell, S. (2000) Communication and Culture: An Introduction. Sage. UK.

Sime, S. (2007) A Practical Approach to Civil Procedure. OUP. UK.

Smith, M. and Kollock, P. (1998) Communities in Cyberspace. Routledge. UK.

Sprenger, P. (1999) Sun on Privacy – Get Over It. Available at: http://www. wired. com/politics/law/news/1999/01/17538

Treacy, B. (2009) ICO Tells Employers – Don’t Be Scared to Screen Staff. Privacy and Data Protection. 10 2 1 2 (December)

Wilkes, A. (2011) What Does Privacy in the Workplace Really Mean in Europe? – Part 11. Privacy and Data Protection. 11 4 14 (March)