



This is a repository copy of *Dimensions of employee privacy: an empirical study*.

White Rose Research Online URL for this paper:  
<http://eprints.whiterose.ac.uk/86714/>

Version: Accepted Version

---

**Article:**

Ball, K., Daniel, E.M. and Stride, C. [orcid.org/0000-0001-9960-2869](https://orcid.org/0000-0001-9960-2869) (2012) Dimensions of employee privacy: an empirical study. *Information Technology and People*, 25 (4). pp. 376-394. ISSN 0959-3845

<https://doi.org/10.1108/09593841211278785>

---

**Reuse**

Unless indicated otherwise, fulltext items are protected by copyright with all rights reserved. The copyright exception in section 29 of the Copyright, Designs and Patents Act 1988 allows the making of a single copy solely for the purpose of non-commercial research or private study within the limits of fair dealing. The publisher or other rights-holder may allow further reproduction and re-use of this version - refer to the White Rose Research Online record for this item. Where records identify the publisher as the copyright holder, users can verify any specific terms of use on the publisher's website.

**Takedown**

If you consider content in White Rose Research Online to be in breach of UK law, please notify us by emailing [eprints@whiterose.ac.uk](mailto:eprints@whiterose.ac.uk) including the URL of the record and the reason for the withdrawal request.



[eprints@whiterose.ac.uk](mailto:eprints@whiterose.ac.uk)  
<https://eprints.whiterose.ac.uk/>

## Dimensions of Employee Privacy: An Empirical Study

Word count = 6,883 (excluding abstract, tables and references)

### Abstract

**Purpose:** The study goes beyond the more frequent interest in information privacy to identify other notions of privacy within the workplace. It seeks to explore how these additional notions of privacy relate to key demographic and employment characteristics and how data protection training, often instigated as a means of highlighting and addressing issues relating to privacy of customers' *data*, is related to *employees' notions of their own workplace privacy*.

**Methodology:** The study was undertaken in two telephone call centres since they offered a working environment where staff are highly monitored and hence there are likely to be issues relating to employee privacy. The study is exploratory in nature and adopts a mixed method approach based on a questionnaire survey that was followed by semi-structured, qualitative face to face interviews.

**Findings:** The survey findings identified three distinct notions of privacy; the concern for personal information privacy (CfPIP), the concern for working environment privacy (CfWEP) and the concern for solitude privacy (CfSP). The findings were supported by the qualitative data provided by the interviews. CfWEP is found to be a gendered issue, with women showing a greater concern for the privacy of their working environment. Finally, the findings indicate that effective data protection training are associated with increased concern for their own privacy in the form of CfPIP, and that inclusion of data protection issues in performance reviews is associated their concern for CfWEP.

**Originality:** Previous studies of privacy in the workplace focus on the simplistic notion of information privacy. This study goes beyond such studies and provides empirically-based evidence of multiple dimensions of privacy operant in a single, real-world workplace setting. It also provides empirical insight to the previously

unexplored issue of the association between data protection training *employees'* notions of their own privacy.

**Keywords:** workplace privacy, information privacy, working environment, solitude

**Type of paper:** Research paper

## **Introduction**

Advancing technology, depersonalisation of the workplace and other *social environments, a growing population...all can be expected to create a greater personal need for a sense of space and dignity* (Erwin Chemerinsky quoted in Smith et al., 1996)

Previous research shows rising levels of concern about privacy of all types (Electronic Privacy Information Center, 2008; McRobb and Rogerson, 2004; Zakaria et al., 2003; Walczuch and Steeghs, 2001). Much of this concern is focussed on the privacy of personal information, and is fuelled by both the widespread use of information systems by organizations to capture, store and process information, and the ease of transmission of information between organisations (Zureik et al., 2010). Although personal information may be given voluntarily by individuals in some situations, significant disquiet exists regarding the collection of information without the explicit knowledge or permission of individuals; for example, during on-line shopping or browsing the web (Turow et al., 2005). The ubiquitous use of a range of surveillance techniques, such as CCTV cameras sited in public places and the monitoring of electronic communication, have resulted in individuals also being concerned about privacy in the wider environment (Clarke, 2001; Electronic Privacy Information Center, 2008; Friedman et al., 2006).

Within the fields of privacy and surveillance studies, much research has focussed on the privacy expectations and experiences of individuals in their daily lives as citizens or consumers. In such cases, objectors may have the opportunity to protect their privacy by refusing to use certain services or go to certain locations; for example, by

not participating in store loyalty schemes that record an individual's shopping patterns, or by avoiding locations with a high density of CCTV cameras (Deighton, 2005; Dommeyer and Gross, 2003). However, whilst individuals may be able to make some choices to protect their privacy as citizens and consumers, it can be harder to take such action in their workplaces, as they will usually be subject to the working practices and environment dictated by their employers. Recognising the importance of privacy to employees, and hence also to employing organisations, research in privacy and surveillance in the workplace is therefore considered important and has been receiving growing attention.

Whilst previous studies have touched upon different facets of privacy in the workplace, the vast majority of research focuses on the concept of information privacy and how it is violated or protected by organizational practices. Very few studies have ventured beyond information privacy in the workplace, an exception being the work of Sundstrom et al. (1980), which explored the notion of 'architectural privacy' in the context of open plan work spaces.

The aims of our study and its potential contributions are three-fold. Initially we seek to go beyond the simple focus on information privacy by identifying and exploring other notions of privacy that are simultaneously operant. We then explore how the notions of privacy identified relate to key demographic and employment characteristics at the level of the employee. Finally, data protection training is often instigated as a means of highlighting and addressing issues relating to information management and privacy, both of customer and employee data. Whilst viewed as important in many sectors and provided widely, previous research has not explored the association between data protection training and the notions of privacy held by employees.

In order to explore privacy, a working environment where issues relating to employee privacy are likely to arise was required. Telephone call centres, where employees work in large open-plan environments and are subject to on-going monitoring and recording, meet this condition and hence formed the empirical setting for this study.

The paper commences with a review of the literature relating to privacy in the workplace. The methodology adopted for the study is then described and the findings are presented and discussed. The paper concludes by noting the limitations of the current study and by suggesting opportunities for future research.

## **Privacy in the workplace**

### Notions of Privacy

Broadly stated, privacy can be viewed as ‘a natural right of free choice concerning interaction and *communication...fundamentally linked to the individual’s sense of self, disclosure of self to others and his or her right to exert some level of control over that process*’ (Simms, 1994, p.316). Many studies recognise the multi-dimensional nature of privacy (DeCew, 1997; Westin, 2003; Burgoon, 1989; Altman, 1975). For example, Zureik (2004) draws on Solove (2002) and others to characterise privacy concepts as clustering around six dimensions, which concern the subject’s rights of solitude, limitation of access, anonymity, information privacy, bodily integrity and intimacy. Within the workplace, solitude relates to the employee’s ability to have times when they are completely alone. Limitation of access (Altman, 1975; Chaikin and Delega, 1974; Warren and Laslett, 1977) is contextualised as the employee’s freedom from being watched or listened to as they work. The subject’s ability to remain anonymous (Altman, 1976; Westin, 1968) concerns employees’ control over whether they are identified by name at particular work times and places; information privacy relates to how employees’ personal information is collected, used and disseminated (Stone et al., 1999). Bodily integrity and intimacy are respectively manifest in a subject’s ability to control access to their body; and to share confidential matters with trusted others.

Despite the apparent diversity inherent within the concept of privacy, the expanding body of literature examining privacy in the workplace tends to focus solely on information privacy, often specifically upon invasive organizational information-gathering practices and processes. For example, information collected during recruitment, particularly that pertaining to the education, family background, personality and medical history of candidates was found to compromise privacy

(Stone and Stone-Romero, 1998). Similar conclusions were drawn about techniques such as medical examinations, polygraphs and honesty tests (Stone-Romero et al., 2003). Rapid advances in the use of email, social networking applications and human resource information systems have raised further concerns (American Management Association, 2001), particularly if systems are breached or hacked (Simon, 2005; Surveillance Studies Network, 2010; Verton, 2004). Employee drug testing and the rise of other biometric measures is another area of concern. Although this is not a practice which is widespread in Europe, except for in safety critical jobs (e.g. driving vehicles), it is commonly used in North America. In a recent development, Microsoft filed a patent for software which can continuously monitor worker well-being through biometric measurements. The patent describes how the system employs wireless sensors to read 'heart rate, galvanic skin response, EMG, brain signals, respiration rate, body temperature, movement, facial movements, facial expressions and blood pressure'. This raises concerns around the right of organizations to probe the 'bodily integrity' of the employee (Zureik, 2004). Commensurate with the views of Miller and Wells (2010), in an organization where these practices proliferate and are pervasive, concerns about privacy may well extend beyond information privacy practices, with the entire working environment being perceived as hostile to employee privacy.

Privacy is an important part of the formal and psychological employment contract, both for employees and employers. For example, it has been linked to procedural justice (Alge 2001; Ball, 2002). Privacy in the workplace is also important in that it has been linked to employee performance. For example, Alge et al. (2006) find that increased empowerment and extra-role behaviours were a direct result of enhanced information privacy perceptions. Nevertheless the dynamics of employee responses to privacy issues is an under explored area, particularly those issues which extend beyond questions of information privacy.

#### Demographic and Employment Characteristics and Privacy

Research findings from studies of privacy in other contexts suggest that employee perceptions of the varying notions of privacy outlined above may vary according to their demographic characteristics. Gender is one demographic variable where a clear

relationship has been found with privacy concerns (Friedman et al., 2006; Kuo et al., 2007; Milne and Rohm, 2000; Paul, 2001; Pedersen, 1987). In consumer research, women exhibited a greater general concern for privacy issues than men (Milne and Rohm, 2000), as well as a greater awareness of their personal information and the protection available (Paul, 2001). In the field of Human-Computer Interaction, Friedman et al. (2006) again found that women had greater privacy concerns in a simulated visual surveillance exercise in a public place. They suggest that the gender difference observed in some aspects of privacy is connected to the differential experiences of women and men in public and open spaces (Pedersen, 1987). Historically, women have shown greater concern for privacy because of unreasonable intrusions upon their privacy in public, for example, through experiencing sexual harassment or being subject to unwanted attention or voyeurism (Allen, 1988). Moving into the world of IS professionals, Kuo et al. (2007) found that women exceeded men in regulatory self-efficacy overall and particularly in terms of whether they protected information and acquired extra information about an individual. In contrast, mixed results are found in studies of the relationship between another demographic variable, age, and privacy concerns (Dommeyer and Gross, 2003).

Considering employment characteristics, several studies have described how individuals' orientation to privacy and ethics influences their engagement with privacy issues in the workplace. Alder et al. (2007) found that an individual's ethical orientation had direct effects on the perceived privacy invasiveness of different human resources programmes, and direct and indirect effects on the perception of the appropriateness of those programmes. Earp and Payton (2006), for example, explored individual 'privacy orientation' in banking and healthcare workers and its influence on their handling of personal data. They demonstrated that these two sectors demanded employees to be oriented to different elements of the data collection, use and retention process.

Sundstrom et al. (1980) explored the concept of architectural privacy in the workplace and found that it was related to job complexity. Architectural privacy concerns how workplace privacy enhancements or violations may be brought about by workspace design. These authors compared the experiences of senior administrators with private offices to less senior clerical and mechanical workers in open plan workspaces and

found that the latter reported greater invasion of privacy because of their working environment. They found that architectural privacy was related to job complexity. Intertwined with notions of job complexity are issues around job tenure and the nature of the job itself (for example, the supervision of others); however, variation in privacy with tenure and the nature of the role has not been explored in previous studies.

### Call Centres and Data Protection Training

We chose to conduct the investigation with employees working in a call centre setting because of the recognised privacy issues therein. The study of call centres and their associated working conditions have been a particular interest for organizational theorists and employment relations specialists over the last decade (e.g. Callaghan and Thompson, 2002; Mulholland, 1999; Taylor and Bain, 2000; Thompson, 2003). These studies have characterised call centre work as repetitive and non-complex (or Taylorised) in nature and often detrimental to employee health and wellbeing (Ball, 2010).

An irony of the call centre environment is that employees who are afforded little privacy themselves are responsible for the privacy of significant customer data, since the rationale and operation of call centres is predicated on employee access to customer information. Training in data protection has been highlighted as important for staff in call centres, due to their handling of customer data, much of which may be sensitive. However, this training may be limited in scope, with Houlihan (2000) highlighting how training activities in call centres are focussed on that which is countable rather than being directly beneficial to performance. Also, such call centre agent training tends to focus on the handling of customer data, rather than considering issues about employee data. To our knowledge, despite the ubiquitous provision of data protection training, linkages between data protection training and employees' notions of workplace privacy have not been explored previously.

In summary, the conceptual basis of this study is drawn from previous studies such as, Zureik (2004), DeCew (1997), Westin (2003), Burgoon (1989) and Altman (1975) that characterise privacy as comprising multiple dimensions. This is combined with the findings from previous studies that suggest privacy orientations are influenced by demographic variables and employment characteristics (for example, Friedman et al.,



2006 and Alder et al., 2007). Finally, the study recognises the salience of data protection training in the call centre environment (Houlihan, 2000) and explores the association between this training and the dimensions of privacy held by employees.

## **Research Questions**

The aims of the research are expressed in the following research questions. Since this research explores previously un-researched aspects of privacy in the workplace, the research questions are purposefully exploratory nature:

1. What are the distinct dimensions of privacy that can be identified in the chosen organisational setting of telephone-based call centres?
2. How do these dimensions of privacy identified relate to the demographic and employment characteristics of employees?
3. How are employees' levels of these dimensions of privacy associated with their training in customer data protection, and the importance of such data protection in their role?

## **Methodology**

### **Research Design**

Consistent with the nature of the study, an exploratory mixed methods research design was adopted. A questionnaire survey was administered to a sample of employees in two call centres, complemented by a series of face to face interviews. One of the researchers was present at each of the two research sites for a week and adopted the role of a non-participant observer. Whilst surveys undertaken on a large scale are often associated with confirmatory studies, suitably designed questionnaires are an accepted means of establishing an initial overview of a new domain of interest or of addressing new research questions. In addition to allowing the previously unexplored view of multiple dimensions of privacy in the single setting of a real-world call centre, the use of an anonymous, self-completed questionnaire as the initial means of collecting data was motivated by a wish to mitigate the possible concerns respondents

may have about providing data about privacy issues, which is often viewed as a sensitive topic.

### Research Setting

The two call centres that formed the basis of the study are both outsourced call centres that is they were operated by an independent provider for a principal firm. One was located in the Western Cape of South Africa (pseudonym SACall) and the other in the South East of the United Kingdom (pseudonym UKCall). Gaining research access to such call centres was exceptionally difficult, due to the highly time pressured nature of their working environment and concerns about what might be found; it took the principal researcher a year to gain access to SACall and three years to negotiate access to UKCall.

SACall was 2 years old at the time of the study and had grown rapidly. All agents worked in an open-plan environment, were subject to stringent electronic and audio monitoring, and were performance-managed and differentially rewarded according to performance. Staff received training on data protection when first joining SACall, and updates on this training during their employment. UKCall was established twenty years ago. Like SACall agents work in an open-plan environment, were subject to stringent electronic and audio monitoring. Data protection training lasted for four weeks and agents were required to pass a written test in order to progress to the phones.

### Survey Instrument

As described previously, gaining access to the research sites was very difficult due to the highly time pressured nature of the work. A lengthy questionnaire would not be acceptable and hence a short questionnaire with a limited number of items was developed. This approach was supported by the high response rates achieved (described below).

In order to further encourage participation, the questionnaire items were drawn from a published consumer survey on privacy (Harris Poll, 2003), which was based on the work of Alan Westin (Westin, 2003). This use of a proven consumer-based survey ensured a set of survey items that were accessible by a wide range of individuals.

Certain items from the poll were excluded due to their lack of relevance to the study. Anonymity was not included due to the systematic absence of anonymity in these workplaces. In both organisations employees were named and identified at all times, either through their access control cards, the name badges they were required to wear, or by their computer log-ins. Items relating to bodily privacy were also excluded because there were no practices in current use by either organisation that threatened bodily privacy. However, we have already acknowledged that such techniques may exist in other workplace settings and these privacy concepts could thus be the focus of a future study. Six privacy items were included in the survey instrument, as shown in Table 1. Respondents were asked to indicate the importance of each according to a five-point Likert scale, coded from 1 “Very unimportant” to 5 “Very important”.

---

INSERT TABLE 1 ABOUT HERE

---

Respondents were also asked to provide basic demographic and employment information, such as age, gender, nature of role and tenure with current employer. Drawing on the Australian Office of the Federal Privacy Commissioner’s (OFPC, 2001), survey of privacy attitudes in business, respondents were asked to rate how effective they found the training they had received in customer data protection and in carrying out their roles according to a five-point Likert scale ranging from 1 “Very ineffective” to 5 “Very effective”. Respondents were also asked to rate how important data protection was in their job description and their performance review according to a five-point Likert scale, coded from 1 “Very unimportant” to 5 “Very important”.

Two further items asked whether respondents had ever withheld their personal information from an employer and if they had ever left a job due to personal privacy concerns (both coded 1 “Yes”; 0 “No”). Qualitative sections were included throughout the questionnaire to allow respondents to expand upon data protection training as well as their experiences of encountering privacy concerns during employment.

Qualitative data were also collected to provide support and depth for the questionnaire findings. This additional data was also seen as important given the pragmatic nature of the survey instrument. Collection of qualitative data was also inspired by Nissenbaum's (2009) elucidation of the importance of context and norms when exploring attitudes towards privacy.

### Population and Sample

The survey instrument was administered by one of the researchers personally handing it to staff. Respondents were given a week to complete the questionnaire, and were asked to place it in an envelope provided and return it to their team leaders or directly to the researcher. Surveys were given out to 80 staff in SACall and 50 in UKCall. A total of 53 questionnaires were returned from SACall and 38 questionnaires from UKCall representing response rates of 66% and 76% respectively, and giving a combined sample of 91 respondents (a combined response rate of 70%). Whilst it is recognised that this is not a large sample, it is consistent with other recent exploratory research in the IS domain (Angeles, 2009: N = 155; Garrido-Samaniego et al., 2009: N = 93; Janvrin et al., 2009: N=72). Consideration was given to non-responder bias; however, given the surveys were distributed across representative teams and there was a high response rate overall, it was considered that this was not a significant issue.

### Statistical Analyses

Statistical analysis commenced with a preliminary check of the independence of the key demographic and employment variables with respect to the location of the call centre, hence justifying the combining of the two sub-samples into a single response sample of N = 91. This was examined using a series of chi-square tests, utilising the  $p < 0.05$  level of statistical significance. Summary statistics were then used to describe the demographic properties of the single response sample.

To address the first research question, Exploratory Factor Analysis (EFA) was used to investigate the existence of and interpret the broader privacy constructs underlying the six items included in the survey instrument. Principal axis factoring was used for extraction, with a scree plot used alongside Kaiser's criterion to identify the number of factors to be retained, and an oblique rotation used to aid interpretation of them, as suggested by Conway and Huffcutt (2003). Having identified the strongest factor

solution, Confirmatory Factor Analysis (CFA) was used to test the adequacy of its fit to the data. Though running CFA on the same sample as EFA is typically sub-optimal compared with a more standard split-half validation that minimises the risk of over-fitting, it was the best option available given the small sample. Similarly, the options available to assess the potentially detrimental effect upon measurement of Common Method Variance (CMV) as described by Podsakoff et al. (2003), were limited by sample size to the use of Harman's Single-Factor Test which suggested that CMV was not an issue. Internal consistency reliability of the resulting groupings ('dimensions') of items was assessed using Cronbach's alpha statistic.

We then calculated an unweighted mean (composite) score for each of the variable groupings to represent each of the emergent privacy dimensions. These scores were used to facilitate the exploration of the second research question, namely the relationships between each privacy dimension and the demographic and employment variables. Given the exploratory nature of the analyses, p values are not reported, rather 95% confidence intervals are provided to indicate where dissimilarity in privacy dimensions existed between demographic subgroups of the sample. Finally, the relationship between each of the three privacy dimensions and the survey items relating to data protection training, withholding information and leaving employment due to privacy concerns were examined using Spearman's rho correlation coefficients.

### Interviews

Interviews were undertaken with a total of 30 staff: 16 in SACall and 14 in UKCall respectively. In SACall 4 team leaders, 2 deputy team leaders and 10 agents were interviewed; in UKCall one project manager and 13 agents were interviewed. The interviews included both staff that had and had not completed the survey.

The interviews were semi structured and covered the following topics: the employee's current role, the nature of the work they performed, the organization's approach to employee and customer privacy. Interviews were transcribed verbatim and coded in NVivo using Boyatzis' (1998) method of thematic analysis. A total of 144 codes were produced which were broadly grouped into role descriptions, an HR bundle (recruitment, training, performance management, job security, promotion, remuneration), privacy, organizational culture, IT infrastructure, personal

development and interviewees' personal histories. Codes relating to information privacy, spatial privacy, privacy importance and privacy problems are drawn upon in this paper to provide additional depth to the findings from the survey.

## **Findings and Discussion**

Summary statistics showed the combined sample to be almost equal in gender distribution (52% male; 48% female), with 39% of respondents aged under 25 and the majority of the rest (a further 42%) between 25 and 34. Sixteen percent worked in a senior position. Overall, only 26% of respondents had worked at the call centre for more than 1 year.

The only evidence of non-independence found between location and demographic and employment variables was with age and tenure. Respondents from SACall were likely to be older and reported higher levels of tenure.

### **Privacy Dimensions**

Two clear factors were identified as underlying the privacy items; together these explained 84% of the variance. Item 6, designed to measure solitude, did not load strongly onto either factor (both loadings < 0.4), and the proportion of its variance explained by the solution was low (communality = 0.26). However this item was retained as a single item for use in measuring solitude in subsequent analyses. The item-factor loadings from the EFA are summarised in Table 2.

Factor 1 was loaded onto by three items that relate to the collection, dissemination and sharing of personal data, and was hence interpreted as 'concern for personal information privacy' (CfPIP). Factor 2 relates to freedom from being listened to or watched in the workplace and is termed 'concern for working environment privacy' (CfWEP). Despite the small number of items in each scale, internal consistency was high, with Cronbach's alpha = 0.892 and = 0.848 for the sets of items representing CfPIP and CfWEP respectively.

---

INSERT TABLE 2 ABOUT HERE

---

Composite (unweighted mean) scores for CfPIP and CfWEP (CfPIP - Mean = 4.21, Std Dev = 1.02; CfWEP - Mean = 3.49, Std Dev = 1.03) indicated that, on average, employees showed greater concern for the privacy of their personal information than the privacy of their working environment. The individual item (6) designed to measure solitude, termed 'Concern for Solitude Privacy' (CfSP), had a mean score of 3.05 (Std Dev = 1.05) suggesting that on average the respondents viewed this as less important than the other types of privacy identified.

Qualitative data supported these findings. Employees spoke without prompting about their concerns about information and work environment privacy but solitude was mentioned to a much lesser extent. These were the only forms of privacy about which they expressed a concern.

Employees had a strong sense of information privacy as they described the information to which they were comfortable with others having access to and which they were not. This appears to support the CfPIP construct. Interviewees were not concerned about access to performance statistics and call recordings by managers, as well as personal data by the HR department, as, for them, this represented normal and legitimate access to their data. They were, however, concerned about what they perceived to be excessive data collection. For example, they objected to email monitoring, as occasionally they sent personal emails. Their responses suggested an implicit boundary around the type of personal information which they believed was acceptable to be collected and used in the workplace and which information they viewed as relating to their non-work life and hence should remain private whilst at work. The following quote from a SACall employee describes this implicit boundary:

*I'm married; I didn't tell work that I was married..... I just have it in my maiden name..... I value the privacy of my home, yeah, that's my privacy....what happens in my house happens in my house.*

A UKCall agent also sought to explore this boundary during the interview:

Our managers get to see a certain amount of our information but when we first started and they were asking us questions, things like do you have a partner, where do you live, *stuff like that, so they obviously don't know as much as maybe I thought they would have known. They don't know our age or anything like that.....*

There was also strong support for the CfWEP construct in the interview responses. For example, a number of interviewees focused on the difficulties of working in an open plan environment. Employees found that the open plan environment helped them learn about call performance but compromised any other form of conversation. A SACall agent described this as:

*I mean you can talk if you want, but you can't really have a personal conversation with six other people listening to you. I'm not like that.*

A number of staff in both call centres identified the use of CCTV in the workplace as unnecessary. A UKCall agent described her dissatisfaction with what she saw as excessive monitoring of her working environment by comparing it to being like an offender in the justice system:

*I am at work, not on day release. I'm already filmed, taped, it is overkill!*

Issues of solitude emerged in a comment from a UKCall agent who noted that the call monitoring they were subjected to revealed the physical whereabouts of employees in the building by showing that they were away from their phones. Employees were only allowed 10 minutes bathroom breaks per day, which was measured via the telephone system. Drawing on military language, this brief comment underlines the lack of privacy felt by a UKCall employee:

*UKCall is so regimented. They even know when we are in the toilet!*

Demographic and employment characteristics



We explored the relationships between dimensions of privacy and demographic and employment variables, with further context provided by statements from the qualitative sections of the questionnaire and interview data. Mean scores for the three types of privacy and key demographic and employment characteristics are shown in Table 3. As can be seen, the only demographic variable for which 95% confidence intervals of group means did not overlap was gender, with females showing a greater concern for CfWEP than males. This finding is consistent with previous literature which examines gender and concern for information privacy issues in various settings, including the workplace (Kuo et al., 2007; Pedersen, 1987; Friedman et al., 2006; Milne and Rohm, 2000; Paul, 2001). It also allows Allen's (1988) assertion that women's experience of public space and privacy is different to be extended to the workplace. The gendered effects of open plan working environments, which are now more likely to feature ambient computing applications, social networking, and electronic communications as well as the more traditional workspace features, therefore need to be addressed as a new form of digital risk (Miller and Wells, 2010). The results also show a greater concern for the other two dimensions of privacy by females. However, the 95% confidence intervals between the mean scores for males and females were overlapping, suggesting that this should be further investigated in a confirmatory study.

Similarly, though confidence intervals once again overlapped, staff with supervisory roles, consistently showed greater concern across all three types of privacy than those with non-supervisory roles, suggesting that their greater exposure to a wider range of data, particularly on employee performance, may make them more sensitive to issues relating to their own privacy. These findings are supported by the qualitative data. The majority of interview respondents raising privacy concerns were team leaders.

Those with greater tenure (which was taken as tenure with the current employer) tended to report lower levels of concern across all three types of privacy. There was a weak positive correlation between those in supervisory roles and tenure (Spearman's  $Rho = 0.24$ ,  $p < 0.05$ ), suggesting in some cases, those that were in supervisory positions had longer tenure, but in many cases that was not so, with the organisations recruiting supervisory staff (which includes team leaders, managers and strategic staff) from outside the organisation. This was particularly true in the case of SACall,

which being relatively new, had to recruit at supervisory levels in order to establish the organisation. When considering tenure, the association of increased tenure with lower levels of privacy concerns could be explained by employees who stay in a post are comfortable with the privacy practices and environment, whilst those that do not will seek to leave.

---

INSERT TABLE 3 ABOUT HERE

---

Table 4 presents the scale mean scores for the three notions of privacy and the correlations of these with items relating to data protection training, withholding information from the employer and leaving a job due to privacy concerns.

The three dimensions of privacy concern share positive correlations, as would be expected given the central theme of privacy, but the size of these correlations is not so large ( $0.27 < \rho < 0.30$ ) as to suggest they are not distinct constructs in their own right.

Positive, medium-sized correlations were also found between personal information privacy (CfPIP) and each of effectiveness of data protection training during induction and during the course of employment, importance of data protection in the job description and importance of data protection in the performance review ( $0.22 < \rho < 0.38$ ). These associations are likely to reflect a virtuous circle as opposed to any definitive underlying direction of causality. Whilst much data protection training is aimed at the management of customer information, such training and emphasis on the importance of customer data privacy is likely to have a ‘spillover’ effect to an individual’s consideration and concern for their own personal information, and that of other employees in the organisation, hence increasing CfPIP. This is consistent with previous studies that suggest a priming effect of data protection procedures (see for example John et al., 2011). Equally, increased CfPIP will cause individuals to recognise the importance of data protection training, and hence is likely to result in them showing greater levels of engagement with the training and rating it as a more important part of their job.

The interview responses underlined how important data protection training and compliance was within both call centres. A team leader in SACall commented:

You can give the wrong opinion, we will give you another chance, but if you fail to *answer data protection questions, we're not going to let you go on the phones. We* make sure that they know the importance thereof before we put them on the phones.

When interviewees in either organization were asked what the consequence of a data protection violation would be, responses varied from *'disciplinary'* to *'dismissal'*. All respondents were aware of this importance and hence had a high awareness of information privacy issues. Data protection compliance permeated every interaction employees had with the customer and their data. It was integrated into call scripts which the employees had to follow and was constantly monitored through qualitative call monitoring which was an integral part of performance review.

In contrast, both CfWEP and CfSP exhibit weaker relationships with the effectiveness of training in data protection (induction:  $\rho = 0.18$ ;  $\rho = 0.10$  respectively, and during employment:  $\rho = 0.13$ ;  $\rho = 0.12$  respectively), and with the perceived levels of importance of data protection in the job ( $\rho = 0.19$ ;  $\rho = 0.21$  respectively). This difference in strength of association lends further support for the discriminant validity of the dimensions of CfWEP and CfWIP (i.e. that CfWEP is a distinct construct from CfPIP). This weaker relationship between CfWEP, CfSP and data protection training dimensions (compared to those shown by CfPIP) is perhaps not surprising. The main focus of data protection training for call centre agents is on the collection and management of customer information. Issues of working environment privacy (i.e. those relating to CfWEP) are only addressed in training in terms of how to manage documents and the use of PCs. For example, PCs should not be left unattended with customer information visible, documents which contain customer information should not be left on printers and copiers and agents should not make notes at their desk).

CfWEP and CfSP resemble CfWIP in their positive associations with the perceived importance of data protection in an employee's performance review. Employees who

are having cause for concern with privacy issues of any type are correspondingly more likely to be sensitive to, and to raise privacy and data protection issues in their performance reviews, enhancing their relative importance and the perception of their importance in the review process. It also reflects the pervasiveness of performance management in call centres, which is reinforced both through electronic monitoring and call recording, as well as the physical presence of supervisors in the open plan workspace. Equally, if privacy issues are already an important part of performance review, then these staff may expect equitable behaviour by their employers and may expect their own privacy in their working environment to be respected.

Counter-intuitively, CfPIP and CfWEP were not found to be positively related to ever having withheld personal information from an employer or having left a job due to privacy concerns (CfPIP;  $\rho = 0.00$ ,  $\rho = -0.11$ ; and CfWEP;  $\rho = -0.04$ ,  $\rho = -0.22$  respectively). Very few qualitative comments were made in interviews concerning this aspect even with the prompting inherent in the semi structured format that was used. This can be understood due to the sensitive nature of the question. However, with the anonymity offered by the qualitative sections of the questionnaire, some respondents admitted to withholding background information from their employer. Some had been economical with the truth about their past if they thought it would be detrimental to their chances of either getting a job or progressing in the organization. A number of mechanisms may be in operation here. For example, whilst individuals' concern about their personal information and their working environment may vary, they realise and accept that they need to disclose a certain degree of personal information required by employers as they enter into an employment contract. Alternatively, it could be that individual's with greater levels of concern for privacy are those also taking preventative action in terms of seeking employment only in workplaces where they are comfortable with the expected privacy practices and working environment.

---

INSERT TABLE 4 ABOUT HERE

---

## Conclusion

This study set out to explore the notions of privacy operant within a single workplace setting and in doing so has made three contributions. First, within the limitations of the study, it has gone beyond the frequent focus on information privacy and has identified three separate notions of privacy that appear robust and distinct. These have been termed: the concern for personal information privacy (CfPIP), the concern for working environment privacy (CfWEP) and the concern for solitude privacy (CfSP). Whilst personal information privacy, working environment privacy (termed architectural privacy by Sundstrom et al., 1980) and solitude have been recognised in separate studies, they have not previously been measured in the same sample, and hence the relationships of these variables and key characteristics of the employee group, have not been consistently established. The construction of these three notions from existing privacy concepts underlines Buchanan et al's (2007) observation that these underlying concepts can combine in different ways in different contexts. We endorse Nissenbaum's (2009) argument which emphasises the importance of context when studying privacy. We call for future studies of privacy in the workplace to take account of a range of issues which go beyond information privacy to consider workspace design, task design and management style as variables.

Second, the findings show that CfWEP is a gendered issue, with women showing a greater concern for the privacy of their working environment. This confirms that the established relationship between gender and privacy concerns found in other fields is operant within the workplace setting. The recognition of the gendered nature of working environment privacy may also be an important, but as yet unexplored, contributor to the low number of women in certain fields or roles, for example, the long running exploration of the '*severe under-representation of women in the information and communication technologies (ICT) labour market*' (Richardson, 2009, p.27) (see also Joshi and Kuhn, 2007; Timms et al., 2008).

Thirdly, the findings suggest that effective data protection training, and highlighting the importance of data protection in both job descriptions and performance reviews, is associated with greater concern for CfPIP and, in the case of the importance in performance reviews, with greater concern for CfWEP and CfSP. This suggests that

during training where the handling of customer data and privacy are addressed, employers should demonstrate that employee data is held in the same high regard, and is worthy of treatment with the same stringent rules and processes.

This study has explored and linked three elements of privacy in the workplace. However, it is recognised that there are additional elements of privacy that are of concern both to employees and employers. Much current interest focuses on the monitoring of emails, text messages and the use of the internet (Lugaresi, 2010; Smith and Tabak, 2009). For example, the Supreme Court in Canada has judged that employers are permitted to track employee text messages sent on workplace electronic devices (Venable, 2010). Such monitoring may be made explicit by means of electronic privacy policies. However, the concern of many is that such monitoring may be covert and can provide very detailed and extensive information on individuals. Whilst it is important to extend studies to the domain of electronic privacy in the future, the findings presented in this paper, particularly the recognition that some elements of workplace privacy are gendered, provide an important starting point for such future studies of these more complex aspects.

### **Limitations of Current Study and Opportunities for Future Research**

It is recognised that the current study was exploratory in nature. Future confirmatory studies would benefit from a larger sample size, which would also allow more detailed and powerful statistical analysis, such as a more rigorous validation of the factor structure underlying privacy dimensions using confirmatory factor analysis. Furthermore, although the study has identified the co-presence of CfPIP and CfWEP in one sample, we recognise that the notion of a ‘working environment’ is a very broad concept which invariably has a number of constituent elements.

The current study, by design, focussed on one industry setting that is recognised as particularly challenging for personal privacy. Future studies could usefully explore the same issues in other sectors in order to identify which aspects of the environment or working practices exacerbate or mitigate issues relating to all three types of privacy identified in this study.

Finally, as discussed above, it would be beneficial both to employees and their employers to extend the privacy concepts identified in this study to newer domains such as the impact of the use of electronic communication technologies and biometrics on concerns for workplace privacy. As working environments become more technologically enabled, it will be important for future research to distinguish the locus of CfWEP, in other words, to what degree the concern emanates from open plan working, widespread email circulation, the use of social networking applications, or even through the use of biometric devices; how these concerns vary across different demographic and employee groups and how concerns about the different dimensions of workplace privacy are related to each other and how those concerns may be mitigated.

## Tables and Figures

**Table 1: Survey Items**

Zureik's (2004) Dimensions of Privacy	Survey Items
Information Privacy	1. How important is it to you to be in control of whether you give out your personal information? 2. How important is it to you to be in control of who can get hold of your personal information?
Intimacy	3. How important is it to you to be able to share confidential matters with trusted persons?
Limitation of Access	4. How important is it to you not to have someone listening to you perform your job without your permission? 5. How important is it to you not to have someone watching you perform your job without your permission?
Solitude	6. How important is it to you to have times when you are completely alone at work?



**Table 2: Item-factor Loadings from Exploratory Factor Analysis**

	Item	Factor 1: Concern for personal information privacy (CfPIP)	Factor 2: Importance of privacy of workplace environment (CfWEP)
1	How important is it to you to be in control of whether you give out your personal information?	0.930	
2	How important is it to you to be in control of who can get hold of your personal information?	0.931	
3	How important is it to you to be able to share confidential matters with trusted persons?	0.856	
4	How important is it to you not to have someone listening to you perform your job without your permission?		0.905
5	How important is it to you not to have someone watching you perform your job without your permission?		0.954
Single Item – does not load onto two identified factors (CfSP)			
6	How important is it to you to have times when you are completely alone at work?		

N = 91. Factor loadings of below 0.5 omitted for clarity

**Table 3: Importance of Personal Privacy by demographic and employment characteristic subgroups**

	Concern for personal information privacy (CfPIP)		Concern for working environment privacy (CfWEP)		Concern for solitude privacy (CfSP)	
	Mean	95% Confidence Interval for mean	Mean	95% Confidence Interval for mean	Mean	95% Confidence Interval for mean
<i>Location</i>						
UK	3.97	(3.57, 4.38)	3.33	(2.97, 3.68)	2.87	(2.58, 3.16)
South Africa	4.38	(4.18, 4.59)	3.60	(3.34, 3.86)	3.19	(2.89, 3.49)
<i>Gender</i>						
Female	4.26	(3.95, 4.58)	3.73*	(3.50, 3.97)	3.13	(2.79, 3.46)
Male	4.16	(3.88, 4.44)	3.23*	(2.96, 3.49)	2.98	(2.71, 3.24)
<i>Age (years)</i>						
15 - 24	4.29	(4.07, 4.50)	3.47	(3.18, 3.76)	2.97	(2.64, 3.31)
25 - 34	4.08	(3.67, 4.49)	3.49	(3.11, 3.86)	3.13	(2.78, 3.48)
35+	4.35	(3.89, 4.81)	3.53	(3.06, 4.00)	3.06	(2.57, 3.54)
<i>Role of staff</i>						
Non-supervisory	4.20	(3.97, 4.43)	3.46	(3.22, 3.70)	2.96	(2.70, 3.21)
Supervisory	4.38	(3.92, 4.84)	3.68	(3.14, 4.22)	3.57	(3.18, 3.97)
<i>Job Tenure</i>						
0 - 6 months	4.35	(4.12, 4.59)	3.51	(3.20, 3.82)	2.85	(2.54, 3.17)
6 - 12 months	4.20	(3.84, 4.56)	3.63	(3.26, 3.99)	3.45	(3.04, 3.86)
1 - 2 years	3.98	(3.38, 4.59)	3.38	(2.94, 3.81)	3.25	(2.85, 3.65)
2+ Years	3.75	(1.93, 5.57)	3.13	(1.51, 4.74)	2.50	(1.52, 3.48)

86 < N < 91

\* 95% confidence intervals for category mean scores do not overlap

**Table 4: Correlations between importance of privacy constructs and data protection training**

	Mean	Std Dev	1	2	3	4	5	6	7	8
1 Concern for personal information privacy (CfPIP) (Min = 1, Max = 5)	4.21	1.02								
2 Concern for working environment privacy (CfWEP) (Min = 1, Max = 5)	3.49	1.03	0.27							
3 Concern for solitude privacy (CfSP) (Min = 1, Max = 5)	3.05	1.05	0.28	0.30						
4 Effectiveness of data protection training during induction? (Min = 1, Max = 5)	4.07	0.94	0.38	0.18	0.10					
5 Effectiveness of this training in data protection during the course of your employment? (Min = 1, Max = 5)	3.95	1.12	0.28	0.13	0.12	0.71				
6 How important a feature of your job description is data protection? (Min = 1, Max = 5)	4.44	0.89	0.33	0.19	0.21	0.48	0.56			
7 How important a feature of your performance review is data protection? (Min = 1, Max = 5)	3.98	1.23	0.22	0.25	0.24	0.45	0.67	0.59		
8 Have you ever withheld personal information from an employer? (1 "Yes", 0 "No")	0.07	0.25	0.00	-0.04	0.07	-0.24	-0.31	-0.11	-0.13	
9 Have you ever left a job because of privacy concerns (1 "Yes", 0 "No")	0.06	0.23	-0.11	-0.22	-0.16	-0.29	-0.32	-0.30	-0.30	0.52

86 < N < 91

## References

- Alder, G.S.; Schminke, M. and Noel, T.W. (2007), "The impact of individual ethics on reaction to potentially invasive HR practices", *Journal of Business Ethics*, Vol 75 No 2, pp. 201-214.
- Alge, B.J. (2001), "Effects of computer surveillance on perceptions of privacy and procedural justice", *Journal of Applied Psychology*, Vol 86 No 4, pp. 797 – 804.
- Alge, B.J.; Ballinger, G.A.; Tangirala, S. and Oakley, J.L. (2006), "Information privacy in organizations: Empowering creative and extra role performance", *Journal of Applied Psychology*, Vol 91 No 1, pp. 221 – 232.
- Allen, A.L. (1988) *Uneasy Access: Privacy for Women in a Free Society*, Rowan and Littlefield, Totowa.
- Altman, I. (1975) *The Environment and Social Behaviour* Wadsworth: Belmont CA
- Altman, I. (1976), "Privacy: A conceptual analysis", *Environment and Behaviour*, Vol 8 No 1, pp. 7 – 29.
- American Management Association (2001) *Workplace Monitoring and Surveillance* New York
- Angeles, R. (2009), "Anticipated IT infrastructure and supply chain integration capabilities for RFID and their associated deployment outcomes", *International Journal of Information Management*, Vol 29 No 3, pp. 219-231.
- Ball, K (2010), "Data protection in the outsourced call centre: An exploratory case study" *Human Resource Management Journal* 20 (3), 2010, p294 – 310.
- Ball, K. (2002) "Categorizing the workers: Electronic surveillance and social ordering in the call centre". In Lyon, D (ed) *Surveillance as Social Sorting* London: Routledge, pp. 201 – 225.
- Boyatzis, R. (1998). *Transforming qualitative information: Thematic analysis and code development*. London: Sage Publications

Buchanan, T. C.; Paine, Joinson, A.M. and U-D Reips (2007). “Development of measures of online privacy concern and protection for use on the internet”. *Journal of the American Society for Information Science and Technology*, Vol 58 No 2, pp. 157 – 165.

Burgoon, J.K.; Parrott, R.; LePoire, B.A.; Kelley, D.L.; Walther, J.B. and Perry, D. (1989). “Maintaining and restoring privacy through communication in different types of relationship”. *Journal of Social and Personal Relationships*, Vol 6, No 2, pp. 131–158.

Callaghan, G. and Thompson, P. (2002), “We recruit attitude: The selection and shaping of routine call centre labour”, *Journal of Management Studies*, Vol 39 No 2, pp. 233-254.

Chaikin, A. and Delega, V. (1974), “Variables affecting the appropriateness of self disclosure”, *Journal of Consulting and Clinical Psychology*, Vol 42 No 4, pp. 588 – 593.

Clarke, R. (2001), “Person location and person tracking. Technologies, risks and policy implications”, *Information Technology & People*, Vol 14 No 2, pp. 206-301.

Conway, J.M. and Huffcutt, A.I (2003), “A review and evaluation of exploratory factor analysis practices in organizational research”, *Organizational Research Methods*, Vol 6 No 2, pp. 147 – 168.

DeCew, J. (1997). *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*, Ithaca: Cornell University Press

Deighton, J. (2005), “Privacy and customer management”, *Customer Management (MSI Conference Summary)*. Cambridge, MA: Marketing Science Institute, pp.17-19.

Dommeyer, C.J. and Gross, B.L. (2003), “What consumers know and what they do: An investigation of consumer knowledge, awareness and use of privacy protection strategies”, *Journal of Interactive Marketing*, Vol 17 No 2, pp. 34 – 51.

Earp, J.B. and Payton, F.C. (2006), “Information privacy in the service sector: An exploratory study of healthcare and banking professionals”, *Journal of Organizational Computing and Electronic Commerce*, Vol 16 No 2, pp. 105 – 122.

Electronic Privacy Information Center (2008), “Public opinion on privacy” available at <http://epic.org/privacy/survey/> accessed December 2010

Friedman, B.; Kahn Jnr, P.H.; Hagman, J, and Severson, R.L. (2006), “The watcher and the watched: Social judgements about privacy in a public place”, *Human Computer Interaction*, Vol 21 No 2, pp. 235 – 272.

Garrido-Samaniego, M.; Gutierrez-Arranz, A. and San Jose-Cabezudo, R. (2009), “Assessing the impact of e-procurement on the structure of the buying centre”, *International Journal of Information Management*, Vol 30 No 2, pp. 135 – 143.

Harris Poll (2003) Most People are Privacy Pragmatists <http://www.harrisinteractive.com/vault/Harris-Interactive-Poll-Research-Most-People-Are-Privacy-Pragmatists-Who-While-Conc-2003-03.pdf> Accessed October 2011

Houlihan, M. (2000), “Eyes wide shut: Querying the depth of call centre learning” *Journal of European Industrial Training*, Vol 24 No 2/3/4, pp. 228–240.

Janvrin, D.; Bierstaker, J. and Lowe, D.J (2009), “An investigation of factors influencing the use of computer-related audit procedures”, *Journal of Information Systems*, Vol 23 No 1, pp. 97-118.

John, L.; Acquisti, A, and Loewenstein, G. (2011), “Strangers on a Plane: Context-Dependent Willingness to Divulge Sensitive Information”, *Journal Of Consumer Research*, Vol 37, No 5, pp. 858-873.

Joshi, K.D. and Kuhn, K.M. (2007), “What it takes to succeed in information technology consulting. Exploring the gender typing of critical attributes”, *Information Technology & People*, Vol 20 No 4, pp. 400 – 424.

Kuo, F-Y.; Lin, C.S. and Hsu, M-H. (2007), “Assessing gender differences in computer professionals self-regulatory efficacy concerning privacy practices”, *Journal of Business Ethics*, Vol 73 No 2, pp. 145 – 160.

Lugaresi, N. (2010), “Electronic privacy in the workplace: Transparency and responsibility”, *International Review of Law, Computers and Technology*, Vol 24 No 2, pp.163-173.

- McRobb, S. and Rogerson, S (2004), “Are they really listening? An investigation into published online privacy policies at the beginning of the third millennium”, *Information Technology & People*, Vol 17 No 4, pp. 442 – 461.
- Miller, C. and Wells, F.S. (2010), “Balancing security and privacy in the digital workplace”, *Journal of Change Management*, Vol 7 No 3-4, pp. 315 – 328.
- Milne, J.R. and Rohm, A.J. (2000), “Consumer privacy and name removal across direct marketing channels: Exploring opt-in and opt-out alternatives”. *Journal of Public Policy and Marketing*, Vol 19, pp. 238 – 249.
- Mulholland, K. (1999), “Back to the future: A call centre and new forms of direct control: ‘slammin’, scammin’, smokin’ and’ leavin’”, 17th Annual International Labour Process Conference, (Royal Holloway College, University of London, London.
- Nissenbaum, H (2009) *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, Palo Alto, CA: Stanford University Press.
- Office of the Federal Privacy Commissioner (OFPC) (2001) 'Community attitudes towards privacy in Australia', Office of the Federal Privacy Commissioner, Australia.
- Paul, P. (2001), “Mixed signals: When it comes to privacy, consumers are fraught with contradictions”, *American Demographics* Vol 72 (23), pp. 45 - 49
- Pedersen, D.M. (1987), “Sex differences in privacy preferences”, *Perceptual and Motor Skills*, Vol 64, pp. 1239 -1242.
- Podsakoff, P. M.; MacKenzie, S. B.; Lee, J. Y., and Podsakoff, N. P. (2003). “Common method biases in behavioral research: A critical review of the literature and recommended remedies”. *Journal of Applied Psychology*, Vol 88, No 5, pp. 879–903.
- Richardson, H. (2007), “Taking a feminist approach to information systems research and using the “thinking tools” provided by the sociologist Pierre Bourdieu”, *Information Technology & People*, Vol 22 No 1, p.. 26 – 35.

Simms, M. (1994), "Defining privacy in employee health screening cases: Ethical ramifications concerning the employee/employer relationship", *Journal of Business Ethics*, Vol 13 No 5, pp. 315 – 325.

Smith, H.J.; Milberg, S.J. and Burke, S.J. (1996), "Information privacy: Measuring individuals' concerns about organizational practices", *MIS Quarterly*, Vol 20 no 2, pp. 167-196.

Smith, W.P. and Tabak, F. (2009), "Monitoring employee emails: Is there any room for privacy?", *Academy of Management Perspectives*, Vol 23 No 4, pp. 33-48.

Simon, K. (2005), *How Technology Can Help, Personnel Today*, May 24<sup>th</sup>, p. 19.

Solove, D. (2002), "Conceptualising Privacy", *California Law Review*, Vol 90, pp.1087 - 1155

Stone-Romero, E.F.; Stone, D.L. and Hyatt, D. (2003), "Personal selection procedures and invasion of privacy", *Journal of Social Issues*, Vol 59 No 2, pp. 343 – 368.

Stone, D.L.; Eddy, E.R. and Stone-Romero, E.F. (1999), "The effect of information management policies on reactions to human resource information systems: An integration of privacy and procedural justice perspectives", *Personnel Psychology*, Vol 52 No 2, pp. 335 – 358.

Stone, D.L. and Stone-Romero, E.L. (1998), "Privacy and human resource information systems", *International Association for Human Resources and Information Management Journal*, II ( 2), pp. 44 – 50.

Sundstrom, E.; Burt, R.E. and Kamp, D. (1980), "Privacy at work: Architectural correlates of job satisfaction and job performance", *Academy of Management Journal*, Vol 23 No 1, pp. 101 - 117

Surveillance Studies Network (2010) *An Update to 'A Report on the Surveillance Society'* Wilmslow: Information Commissioners Office.

Taylor, P. and Bain, P. (2000), "An assembly line in the head: Work and employee relations in the call centre", *Industrial Relations Journal*, Vol 30 No 2, pp. 101-117.

Thompson, P. (2003), "Fantasy Island: A labour process critique of the age of surveillance", *Surveillance and Society*, Vol 1 No 2, pp. 138-151.



Timms, C.; Lankshear, C.; Anderson, N and Courtney, L. (2008), “Riding a hydra. Women ICT professionals’ perceptions of working in the Australian ICT industry”, *Information Technology & People*, Vol 21 No 2, pp. 155 – 177.

Turow, J.; Feldman, L. and Meltzer, K. (2005), “Open to exploitation: American shoppers online and offline”, Annenberg Public Policy Center of the University of Pennsylvania, June 1<sup>st</sup>.

Venable LLP (2010), “Supreme Court upholds employers’ right to monitor text messages”, *Nonprofit Business Advisor*, Issue 251, pp. 6.

Verton, T. (2004), “Email glitch exposes flaw in privacy law”, *Computerworld*, Vol 38 No 28, pp. 1.

Walczuch, R. and Steeghs, L. (2001), “Implications of the new EU directive on data protection for multinational corporations”, *Information Technology & People*, Vol 14 No 2, pp. 142 – 162.

Warren, C. and Laslett, B. (1977) “Privacy and secrecy: A conceptual comparison”, *Journal of Social Issues* Vol 33 No 3, pp 43 – 51.

Westin, A.F. (1968) *Privacy and Freedom*, Athenaeum, New York, NY.

Westin, A. F., (2003). “Social and Political Dimensions of Privacy,” *Journal of Social Issues*, Vol. 59 No. 2, pp. 431-453

Zakaria, N.; Stanton, J.M. and Sarkar-Barney, S.T.M. (2003), “Designing and implementing culturally-sensitive IT applications: The interaction of culture values and privacy issues in the Middle East”, *Information Technology & People*, Vol 16 No 1, pp. 49 – 75.

Zureik, E with L. Lynda Harling Stalker, Emily Smith, David Lyon and Yolande E. Chan (2010) *Privacy, Surveillance and the Globalization of Personal Information: International Comparisons* McGill University Press, Montreal.

Zureik, E. (2004) ‘Globalisation of Personal Data Project: International Survey Concept Paper.’  
[http://www.surveillianceproject.org/files/concept\\_paper.pdf](http://www.surveillianceproject.org/files/concept_paper.pdf) accessed November 2004.