Employee Privacy at Workplaces: Some Pertinent Issues

Sandeep K Krishnan
Biju Varkkey
Anush Raghavan

W.P. No. 2006-02-04
February 2006

INDIAN INSTITUTE OF MANAGEMENT
AHMEDABAD-380 015
INDIA

Employee Privacy at Workplaces: Some Pertinent Issues

- **Sandeep K. Krishnan, Doctoral Student, Fellow Programme in Management, Personnel and Industrial Relations Area, Indian Institute of Management Ahmedabad, sandeepk@iimahd.ernet.in**
- **Biju Varkkey, Assistant Professor, Personnel and Industrial Relations Area, Indian Institute of Management Ahmedabad. bvarkkey@iimahd.ernet.in**
- **Anush Raghavan, Student, Post Graduate Programme, Indian Institute of Management Ahmedabad, 5anushr@iimahd.ernet.in**

⊗ This working paper is a modified version of a paper selected for the presentation at the International HR Conference to be held from February 15-18, at the Indian Institute of Science, Bangalore. The paper is part of a larger research project on employee working conditions and rights. Please do not quote the paper without permission from the authors.

Abstract:

Employee privacy at the workplace is an issue of debate worldwide. With data security and other organizational interests becoming paramount, the employee rights for privacy and freedom is curtailed. This paper explores the underlying factors that contribute to violation of workplace privacy, the factors that affect how workplace privacy is defined, and debates on how privacy notions change based on cultural differences. We also try to understand the relevance of employee privacy nuances in the Indian context. The paper poses pertinent questions on definition of workplace privacy, and the balance of managing the employee and employer interests.

Keywords: Workplace privacy, employee rights, human resource management, recruitment, performance tracking, appraisals, electronic surveillance

Introduction:

Privacy[1]

a : the quality or state of being apart from company or observation **:**
b : freedom from unauthorized intrusion

Employee privacy is a much debated issue in the current context of increasing internet usage, email at work, data security, employee thefts and electronic surveillance of work places. Employee privacy issues have been explicitly brought out in countries like USA where invasion of privacy is considered to be a major infringement of individual rights. There is considerable degree of explicitness that is guaranteed by the law in the context like US for the employee to contest invasion of privacy (For example: Electronic communication privacy act[2]). However in a country like India where we consider data security as paramount and when there is a growing concern about loss of data security, more focus is brought on increasing employee surveillance thus hampering employee privacy further. In this paper the major focus would be to example the possible avenues where HRM practices can hamper employee privacy and how organizations may evolve or will be forced to evolve in the future with special reference to cross cultural differences.

Misuse of vulnerability:

Studies point towards the state of inequality in power in a contractual relationship like that of an employee-employer. As a result it is quite possible for employer to extract more information/publicize information from an employee without his or her full hearted interest or participation (Nye, 2002). The information may be pertaining to the personal life, specific choices, family issues, background, habits etc. that a person might not be willing to disclose to an unknown person/institution knowingly or unknowingly.

Halcrow (2002) brings out some of the possible situations where employee's private matters are being discussed without considering his/her interests. For example, Boss asking an employee to disclose family issues of another colleague who is a friend of the employees and further using it against the colleague or spreading the same in the office, asking an employee suddenly to open his/her wallet to check for possible theft in front of other employees, asking a candidate who is appearing for an interview difficult questions regarding his/her private/ professional life, exposing private messages sent through email to a wider audience and causing embarrassment to the employee etc. The fact to be remembered here is that the organization that might have higher power in the contractual relationship is infringing the employee's privacy and thus on his/her individual rights.

Employers state number of reasons for employee surveillance like improving employee productivity, selecting and retaining honest employees, evaluating employee performance, and even conforming to privacy obligations regarding business contracts. However looking from another angle, increased surveillance leaves no room for employee self control and self monitoring. An employee who is no longer trusted by his employer and vice-versa creates a culture where employee sees no incentive for being productive, resourceful and efficient (Kovach, Jordan, Tansey and Framinan, 2000).

Human resource management and privacy:

Extending the dictionary definition of privacy, employee privacy can be defined as the "Freedom for employees from unauthorized intrusion from employers" or in the US context it is widely understood as "the general right of the individual to be let alone" (Bennett and Locke, 1998). However it is intriguing and would be difficult to segregate what level of information can be

[1] Marriam-webster (dictionary)
[2] http://cio.doe.gov/Documents/ECPA.HTM

sought or demanded that is needed for the organizational business purposes and how far it can be done. The various human resource management practices like recruitment, performance appraisal, employee discipline management and adherence to code of conduct, exit interviews and business operation processes like data security and performance monitoring are potential areas where employee vulnerability can be misused. May be many of the issues would be highly contextual. An interesting example in the Indian context is linked to the queries that employers generally face regarding the authenticity of employee's records for marriage proposals. Though such issues may be amusing in a western culture, organizations in India take different approaches to deal with such issues. For example when a similar issue was posed in front of a group of HR managers, few suggested that "facts regarding an employee can be shared", "it is beneficial for the employee too", and few remarked that "our organization has strict policy regarding non disclosure of employee records". It would be interesting to understand what would be the level of general agreement amongst various organizations.

Recruitment and selection:

Recruitment and selection is one of the critical areas where potential employers can possibly exploit the candidate's helplessness. Few of the possible intrusions mentioned in the western and oriental context are,

- Asking the employee to disclose confidential information about the past employer's
- Asking personal questions like "whether you have a girlfriend/boyfriend?", " Reason's for marriage failure?" "Asking a married person whether he/she is planning to have baby in the near future?" – Clearly these questions may have some relevance for a position fit of the individual to a job. However they clearly violate the individual rights of a person to have privacy to his/her personal/professional life.
- Requesting information about a person from sources that are not in the reference list of the resume of the individual.
- Asking unwanted questions about his/her financial background, caste and family status.
- Asking questions in job application forms that are discriminatory and possibly private matters.
- Sharing of personal information of the employee to third party for background checking/ reference checking.

An organization might see some relevance in the information. However the big question is whether these questions are relevant to the job he/she will be doing and if at all provided will the information provided be kept confidential. Stone-Romero, Stone, and Hyatt (2003) have found that invasiveness of the selection procedure is a critical factor. The study stressed on the importance of the information asked on the subsequent job performance. The paper noted that in case of unwanted information seeking, eligible applicants may be discouraged to apply as they may see it as unwanted invasion of privacy. This might also be a critical factor in discriminating against certain group of eligible applicants.

An example of use of explicit privacy policy while collecting employee details is that of IT major, Dell as given in Appendix 1.

Performance Tracking

Performance appraisal clearly involves monitoring/tracking of employees performance and one to one interactions and discussions to understand how the employee is performing, development areas, and future actions. However this discussion may go beyond what is happening at the work place to understand the probable reasons to find out why an employee is performing badly or showing deviant behaviors. In case of new age industries like BPOs; call monitoring, desktop tracking, and other electronic monitoring mechanisms are widely used to track on job performance, work habits and client management. These activities clearly restrict any possible misuse of organizational resources but also give the possibility of tracking personal conversations

and messages of employees. Literature discusses about how off duty conduct of an employee affects the employer, not just in performance but in areas like corporate image and even legal liabilities arising out of the interactions. In many situations, it is difficult to define where the duty or the organizational responsibilities of an employee end. Some organizations go to the extend to even defining employees personal life choices like what to eat/drink (softdrink companies are famous for it) or where to live. In the recent past, an employee of the Indian Arm of a well known MNC resigned from the job when there was criticism about the particular employee using internet "blogs" as a medium to expose another institution that had business interests with the employer. There are legal view points like "The employer is not the custodian of the griever's character or personal conduct. However, his conduct is a concern to the employer if it adversely impacts on the legitimate business interests of the employer" (Davis and Company document, 2000). In this case the griever is in a similar position as that of the employee mentioned above. These general descriptions of legal conduct hints towards the possible chances of an employer using disciplinary actions against the employee in an event of actions of the employee that are private but are harmful to the employer's business interests.

Electronic Surveillance

While debating on the issue of privacy at workplace, it is impossible to ignore the case of electronic surveillance. In a recent survey by American Management Association (AMA) in 2005, nearly three-fourths of the companies admitted to have been exercising some form of electronic surveillance over their employees (AMA, 2005). That figure is a 27% increase as compared with a similar survey conducted in 2001. Understanding of the term 'electronic surveillance' greatly varies with the context in which is it used (US FISA & NOCO), but in a workplace scenario, it can be said to mean a broad range of monitoring activities by the employer with the aid of electronic tools.

For employers, electronic means of communication poses yet another challenge because of two major factors as put forth by Finlay and McKinlay (2003). First major cause of worry is that employees can get into unintentional sharing of intellectual property rights, infringe copy rights, and leak confidential information, or unintentional contractual liabilities via email or other electronic communication. Also, the exchanges made through email can lead to violation of the norms of organizational membership. Companies are often bound by local laws and regulations governing sexual harassment and work environment, which compel them to monitor employee activity. Employers are responsible for the actions of their employees during the time of employment and thus, it is in their interest to prevent any such activity which may give rise to punitive penalty or embarrassment. The Chevron incident is one such case wherein the "*company had to pay $2.2 million to four plaintiffs who claimed to receive sexual harassment through e-mail jokes from other employees in the company"* (Lee and Kleiner, 2003).

Thus, while it has been established that surveillance and monitoring have been an inescapable feature of work, what makes us pay special attention to it now? Before we answer that question, let us take note of another statistic. In the AMA study, 28% of the surveyed organizations have fired employees for, in that case, abuse of telecommunications equipment. (Lee and Kleiner, 2003). Thus, the fallout of Electronic Surveillance can now have consequences beyond the nature of violation of privacy rights. It is the emergence of new technology which places sophisticated monitoring tools at an affordable price into waiting hands (Vorvoreanu and Baton, 2000 in Johnston and Cheng, 2002). Fostered by lack of relevant legislation, the technologies are exposing the individual worker to scrutiny as opposed to the earlier prevalent group evaluation. Hence, what separates the traditional from new age monitoring is that, "earlier people usually knew when the boss was there; electronic monitoring can be there all the time." (Wen and Gershany, 2005). More often than not, the employee is either unaware of being under surveillance, or in certain cases is oblivious to how the data gathered about his activities is going to be used.

Interestingly electronic monitoring can go to any extent where technology is the limit. Hartman (2001) mentions few of them like internet usage monitoring, access blocking, observing downloaded files, chat monitoring, truth phones (that can tell whether the person on other end is speaking truth), pocket recording pens, monitoring of phone calls using remote computers, etc. Computer based monitoring can be key stroke monitoring (copies and tracks all key strokes made on the monitored computer), email scanning, event logging (lists events happened on the computer chronologically), remote desktop viewing (takes snapshot of the desktop on a periodic basis), application usage (monitors and logs all applications used), and window activity (records all usage in the computer and key stroke monitoring) monitoring (Wen and Gershany, 2005).

On legal grounds, there is little a person can do when his privacy has been breached. In the absence of a specific privacy law, the courts do not offer much protection. The reasoning for this is that, in India as well as most other countries, the right to privacy is a matter of law of torts, the law dealing with a civil wrong. According to law of tort, an action for breach of privacy cannot be brought when the person has a reasonable expectation of privacy. However, the courts are generally not receptive to employees' claims that their work environments contain sufficiently private spaces for an intrusion on seclusion to occur (Workrights.org).

In India the Supreme Court has recognized that the right to privacy is enshrined in A.21 of the Constitution (Kharak Singh vs State of UP, 1 SCR 332 (1964)) but it being a fundamental right is ineffective for the purpose of bringing an action against a private body.

Inevitably, technology will be able to breach all possible individual privacy without the person actually being able to understand the situation. Though restricting personal use of organizational resources and reducing liability of the business due to misuse are widely quoted reasons of monitoring, another fair angle to it would be the question that how can a individual manage his normal routine of life unless he spends some time of work for personal life activities. An example would be scheduling an appointment with a doctor by calling from the office.

Issues and concerns in privacy management:

Privacy management poses significant questions and dilemmas to management and employees. For example in case of IBM that had implemented clear policies regarding employee privacy as early as in the 70's speak about dilemmas like employee privacy information spreading through informal channels, withdrawal of managers to share open relationships with employees and colleagues for the fear of actions against possible privacy violations, linking up privacy with concept like open office spaces, confusions about humanitarian considerations Vs privacy matters, and information that are of business interests Vs confidentiality of private matters (Cary, 1976 (Interview)). Some of the key recommendations from at a generic level are to establish clear policies on workplace privacy, keeping employee medical information confidential, and staying out of employees' personal lives (Halcrow, 2002). The key is to clearly define what privacy means to the organization based on the organizational culture, business needs, and context of the country of operations.

Privacy violations can be directly linked to justice violation and can have number of detrimental outcomes. Examining the effect of privacy invasion, studies have pointed towards lesser organizational commitment and increased deviance as means of employee retaliation. Drawing from the psychological contract literature, privacy invasion might be treated as a form of contract violation and will be associated with employee alienation. However a large number of law suits have been filed in the western context against employers for violating employee privacy concerns and might be the future trend in the Indian organizations.

The other pertinent issue regarding privacy is the very definition of the same. There is a huge variation in understanding privacy based on national culture, organizational culture, HRM policies and even family upbringing. Whitman (2004) discusses at length the differences between

American and European notions of privacy. For example discussing salary is considered normal in an American context and but is considered an invasion of privacy in the European context. Such differences cause unforeseen difficulty in dealing with cross cultural situations. The issue posed in front of a policy maker is that although privacy is a universal concept, what constitutes privacy is more contextual. For example in the context of Indians who are exposed to a different societal culture as a part of work/other engagements try to imbibe notions of privacy that are different from the home culture. Clearly the mismatch and may be a higher degree of valuation for privacy can lead to conflicts both during the exposure to an alien culture and readjustment to the home culture. This might be an area of concern for organizations that have to send their employees to foreign countries as part of business requirements.

Hartman (2001) refers to some of the demands by privacy proponents and trade unions. The message is that monitoring should be limited to workplace, should not cause physical or psychological harm, advance warning should be given, mutual agreement should be present and no secret monitoring is to be done, monitoring in private places like restrooms should be strictly avoided, and only job related monitoring is to be done. The crux is that monitoring should follow the ethical norms of the society. Findlay and McKinlay (2003) also states the importance of having a collective understanding of privacy norms at the workplace level to include the business needs and the organizational contextual understanding. In the Indian context, not many trade unions have clearly voiced the privacy violation issues. However some of the issues like "good conduct" agreements that curtail employees' freedom have been fiercely debated by unions. In the future workplace privacy might be an area where unions would have a point of serious debate.

The other major issue to be dealt with is who has the right to keep the information in the organization. For example there are organizations that want to keep HR managers neutral that they do not give away personal information of employees. Few organizations have policies that restrict marriage of HR personnel with line managers or even discourage office romance in this regard. The issue that is raised is protection of privacy as HR personnel have records of professional and personal background of employees. Also with the extensive use of human resource information systems, the data stored is also available easily. Oz (2001) mentions the possibility of unethical usage of information systems data by IS professionals as a deviant behavior. Clearly the issue would be how privacy policies can be strictly implemented and communicated it to all the employees.

Directions for future research and policy makers:

For research on privacy in the context of India, we would like to pose two major questions. a) What is considered private for a typical employee in India? and b) What are those matters that are considered part of organizational privacy and information that an individual has to forgo as part of his membership in an organization?. Clearly in the Indian context it would be difficult to generate legal systems to support a generic cause of employee privacy. The need would be for organizations to draw lines on the information needs and formulate policies for supporting privacy. Another interesting point would be look at how globalization and growth of multinational organizations would determine workplace privacy with convergence of human resource management practices

Appendix 1:

Dell's Privacy Policy: Information regarding applying for a position

By submitting your Candidate Data to Dell, you understand and agree that:

- **You have reviewed this Privacy Statement;**
- **Dell may process your data in accordance with this statement;**
- **Your data may be transferred to other Dell locations worldwide (subject to applicable law).**

This policy applies to data submitted by any method to DELL in connection with a job application, including online questionnaires and applications received via regular mail or hand delivery.

Principles

- Data will be collected lawfully and processed strictly for the purposes specified below and used accordingly.
- Data will be adequate, relevant and not excessive relative to the purposes for which collected and processed.
- Data will be as accurate and up-to-date as possible.
- Data will not be kept longer than appropriate or necessary for the purposes for which processed or as legally required.
- Data will be collected, used and retained in accordance with legal rights.
- Data will be protected by appropriate security measures to prevent unauthorized access, or accidental loss or damage.

Processing

- Processing includes, but is not limited to, obtaining, organizing, recording, maintaining, transferring, using, disclosing, disseminating or otherwise making available, blocking, destroying and erasing Data.

Candidate Data

Candidate Data that is processed includes:

- Candidate status
- Personal data, such as name, age, telephone numbers, addresses
- Work history/job data
- Education
- Compensation
- Employer feedback
- Online questionnaire results

Sensitive Candidate Data also may be processed in accordance with local law, where necessary and permissible (including obtaining express consent, if required) and includes:

- Financial data;
- Medical or health data;
- Demographic data, such as gender, race, religion, national or ethnic origin, political affiliations, criminal proceedings, or membership in trade unions.

Use of Third Parties

- Subject to local laws, DELL may use third party service providers to collect, process and/or validate Candidate Data.
- These service providers are required to ensure adequate protection for Candidate Data and to comply with local laws.

Disclosure

DELL may disclose certain Candidate Data in accordance with applicable laws to:

- A third party service provider in connection with the use and processing of Candidate Data;
- Others, such as governmental authorities, in order to protect the interests or rights of DELL or third parties.

Transfer

- DELL may process and transfer Candidate Data to other DELL locations outside your

country or region for purposes relating to its global business operations, including human resources planning and reporting requirements;

- The process, transfer, and release of Candidate Data within DELL and/or to third parties outside your country is subject to local law, including, where required, obtaining consent, and involves utilizing adequate security measures.

Security

- DELL has implemented reasonable and adequate security measures to protect manual and electronic processing of Candidate Data and prevent misuse.

Access

If your Candidate Data is held electronically as a result of the submission process or completion of an online questionnaire:

- You may view and/or correct your Candidate Data (subject to applicable local legal limitations and requirements).
- Requests for access, correction, feedback, withdrawal of consent or other questions must be addressed in writing to Dell's Human Resources department.
- The Dell Human Resources department will confirm your rights of access to such Candidate Data.
- The retention and access to Candidate Data shall all be in accordance with applicable local legal requirements.
- You are encouraged to make sure that Candidate Data is kept current and accurate.

Resolution

- DELL will endeavour to resolve any issues concerning your Candidate Data in accordance with relevant procedures and policies as well as local laws and requirements.

References:

Bennett, S.C., & Locke, S.D. (1998). Privacy in the workplace: A practical primer. *Labor law Journal*, 49(1): 781-788.

Cary, F.T. (1976). IBM's guidelines to employee privacy. *Harvard Business Review*, 54(5): 82-91.

Davis & Company. (2002). Privacy issues in the workplace-"Employee off-duty activities".

Findlay, P., & McKinlay, A. (2003). Surveillance, electronic communications technologies and regulation. *Industrial Relations Journal*, 34(4): 305-318.

Halcrow, A. (2002). Navigating the new landscape of workplace privacy rights. *Employment Relations Today*, 29(1): 49-53.

Hartman, L.P. (2001). Technology and ethics: privacy in the workplace. *Business and Society Review*, 106(1): 2-27.

Johnston, A., & Cheng, M. (2002). Electronic surveillance in the workplace: Concerns for employees and challenges for privacy advocates. *Paper Delivered – International Conference on Personal Data Protection*, Seoul Korea.

Kovach, K.A., Jordan, J., Tansey, K. & Framinan, E. (2000). The balance between employee privacy and employer interests. *Business and Society Review*, 105(2): 289-298.

Lee, S., & Kleiner, B.H. (2003). Electronic surveillance in the workplace. *Management Research News*, 26(2/3/4): 73-81.

Nye, D. (2002). The privacy in employment critique: a consideration of some of the arguments for 'ethical' HRM professional practice. *Business Ethics: A European Review*, 11(3): 224-232.

Oz, E. (2001). Organizational commitment and ethical behavior: An empirical study of information systems professionals. *Journal of Business Ethics*, 34: 137-142.

Stone-Romero, E.F., Stone, D.L., & Hyatt, D. (2003). Personnel selection procedures and invasion of privacy. *Journal of Social Issues*, 59(2): 343-368.

Wen, H.J., & Gershuny, P. (2005). Computer based monitoring the American workplace: Surveillance technologies and legal challenges. *Human Systems Management*, 24: 165-174.

Whitman, J.Q. (2004). The two western cultures of privacy: dignity versus liberty. *The Yale Law Journal*, 113(4): 1151-1221.

Weblinks:

Electronic Monitoring in the Workplace: Common Law & Federal Statutory Protection. Retrieved 25 January, 2006 from http://www.workrights.org /issue_electronic/em_common_law.html

Privacy and human rights 2003: Country reports. Retrieved 25 January, 2006 from http://www.privacyinternational.org/survey/phr2003/countries/india-footnotes.htm#ftn1468

Dell India: About Dell. Retrieved 25 January, 2006 from http://www1.ap.dell.com/content/topics/topic.aspx/global/hybrid/careers/content/7c211fd2-a405-4810-afbf-709d3c7646a7?c=in&l=en&s=corp