IMPACT FACTOR 3.47

ISSN 2349-1027

International Registered & Recognized Research Journal Related to Higher Education for All Subjects

INDO WESTERN RESEARCHERS

UGC APPROVED & PEER REVIEWED RESEARCH JOURNAL

Issue : X, Vol. V

Year- V, Bi-Annual(Half Yearly)

(Feb. 2018 To July 2018)

Editorial Office :

'Gyandev-Parvati',

R-9/139/6-A-1,

Near Vishal School,

LIC Colony,

Pragati Nagar, Latur

Dist. Latur - 413531.

(Maharashtra), India.

Website

www.irasg.com

Contact : - 02382 - 241913

09423346913 / 09637935252

09503814000 / 07276301000

E-mail :

visiongroup1994@gmail.com

interlinkresearch@rediffmail.com

mbkamble2010@gmail.com

Published by :

Indo Asian Publication,

Latur, Dist. Latur - 413531 (M.S.)India

Price : ₹ 200/-

Indo Western Researchers (IWR) (1)

IMPACT FACTOR 3.47

ISSN 2349-1027

Indo Western Researchers (IWR)
Issue : X, Vol. V
Feb. 2018 To July 2018
www.irasg.com

Research Paper 1 Commerce

Information Privacy in an Organization

Dr. Prakash Kadrekar
Dept. of Commerce,
Degloor College,
Degloor, Dist. Nanded (MS) India

ABSTRACT

With descriptives like "the information age," "the information super highway," and "the knowledge economy"-popular in the mainstream business literature at the start of the 21st century-there can be little doubt that information plays a vital role in the success of any organization. Employees often are required to sign nondisclosure agreements upon entry into an organization wherein they vow that they will not divulge proprietary company information to outsiders. Such safeguards seem reasonable and are becoming necessary for organizations interested in protecting their assets-specifically, their intellectual assets-from getting into the hands of competitors or other entities that could misuse that information. Information is a broad concept, however, and the need for organizations to acquire and subsequently protect information is not limited to patents, "know how," organizational routines and technologies, and other intellectual property. Organizations also have a need to acquire and protect information about human assets, that is, their employees-the very people who will be entrusted to help the organization succeed. The gathering of employee personal information is dramatically on the rise and the mechanisms through which information is gathered are diverse and controversial.

Keywords: Disclosed Matters, Legal Information, Security issues, Unending Information.

Introduction:

Organizations have to be careful about how they gather and protect information, because as they attempt to gather personal information

through various means, there is the potential to impinge on employees' sense of information privacy. Information privacy is defined as an employee's belief in his or her ability to control information about him- or herself and his or her resulting ability to act autonomously free from the control of others (Stone & Stone, 1990). Information privacy, therefore, reflects an important psychological state influenced jointly by an organization's need to collect personal information on one hand and an individual employee's desire to maintain control over his or her personal information on the other hand. This constant tension between the organization and the individual over personal information also suggests that information privacy is part of dialectic process or struggle.

In his 1975 book, The Environment and Social Behaviour, Altman argued that privacy represents a boundary-regulation process wherein individuals regulate their interpersonal boundaries with each individual varying in both desire for openness and closeness and ability to reach desired levels of openness and closeness. These needs parallel similar needs in the general psychology literature, including the need for affiliation or belonging and the need for distinctiveness.

There are times in one's work life, for example, where one wishes to close oneself off from others or to be separate or distinct (e.g., shutting the door to one's office; not answering phone calls). To the extent that people can achieve their desired level of closeness, privacy is maintained. Similarly, there may be times where the same employee desires social interaction with co-workers or to be open to others (thus satisfying broader needs for affiliation and belonging). He or she might invite such interaction, for example, by leaving the door open or working in a common area, and to the extent other employees stop by, privacy control is maintained. In this situation, privacy is not threatened because the interaction with others was desired and achieved. If, however, no co- workers stop by to visit when such visits are desired, a privacy void occurs insofar as individuals are experiencing unwanted seclusion. Both psychological goals-desire for openness and desire for closenessexist along a continuum, and people struggle to achieve an optimum level. Moreover, one's optimum level may not remain static (i.e., the perceived boundary between the self and others and the desire for openness and closeness are fluid).

Employees are conscious of their own privacy boundaries and the actions of organizations aimed at gathering their personal information. When such organizational aims are irrespective of those boundaries, significant tension can result. That is, the need for an organization to collect employees' personal information to improve organizational security is frequently in conflict with employees' desires to maintain control over their personal information. Because of this tension and the growing number of ways-techno-logically and otherwise organizations are able to monitor employees and

collect information about them, the battle for personal information is becoming an increasingly important managerial dilemma that can no longer be easily discounted.

What Organizations Are Doing: Information Gathering and Privacy Trends:

Employers must protect their assets, but how far should they intrude into the privacy of their employees in order to accomplish this goal? Employees have rights of privacy, or as Warren and Brandeis (1890) articulate, the right to be let alone, that must be respected, but research also indicates that intrusive electronic and other forms of monitoring might have unintended psychological consequences on employees that can hurt both employees and employers in the long run. In this section, some of the specific trends and emerging technologies that potentially pose privacy threats to employees are discussed.

Electronic Performance Monitoring:

Electronic performance monitoring, or EPM, refers to the gathering and processing of information about employees to measure employee performance (Aiello, 1995; Alder, 2001). EPM is commonly used in office settings because the nature of office work increasingly involves the use of computers; EPM can be used to track employee behaviors including keystrokes, Web sites visited, and e-mails created and sent. However, EPM is not limited to computers it can take place by way of other electronic devices, such as telephones, video monitors, and global positioning systems (GPS). Consider the results from a 2005 American Management Association survey on electronic monitoring:

Web and Internet Monitoring-

- 65% of employers block certain Web sites-a 27% increase from 2001
- 76% of employers monitor employee Web surfing
- 26% of employers have fired employees for inappropriate use of the Web or e-mail
- 36% of employers track computer key-strokes
- 50% of employers regularly review total computer con-tent-this is up from 36% in 2001
- 55% of employers retain employee e-mails and review them regularly-this is up from 8% in 2001

Telephone Monitoring-

- 57% of employers now block certain lines on their employees' phones
- 51% of employers now keep track of how long their employees talk on the phone, and about half of these tape and review employee voicemail-this is up from about 12% in 2001
- 6% of employers have fired employees for phone misuse

Video Monitoring-

- More than 50% of employers video monitor their employees (up from 33% in 2001)
- 10% of employers video monitor for performance purposes
- 6% videotape all their employees

Global Positioning Systems (GPS) Monitoring-

- 8% of employers use GPS to track employee ID cards
- 8% of employers use GPS technology to track employer-owned cars

A burgeoning market of effective and inexpensive technology has made EPM a feasible and readily available tool for most employers.

Personality and Workplace Testing-

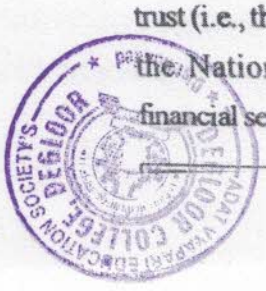
Workplace testing has become very common in the 21st century (nearly half of employers administer such tests equating to several million tests each year), and increasingly reliable tests are being developed by researchers to measure individual differences. Workplace tests are often used in the employee selection process to help identify reliable and trustworthy employees who "fit" the organization. Personality tests, for example, are commonly used by employers to help determine whether a potential employee has personality problems or serious emotional disturbances that may adversely affect job performance-related outcomes, and whether the person will fit within the company's culture. Similarly, integrity tests are often employed to identify potential employees who are likely to engage in theft or other antisocial behaviour. Certain organizations, where the confidentiality of information is part of the core business process, have a special interest in hiring people they can trust (i.e., the Central Intelligence Agency [CIA], the National Security Agency [NSA], and financial service companies). These organizations make integrity testing an integral part of their employee-selection process.

Despite their usefulness to organizations, workplace tests are often criticized. Some argue that integrity tests ask questions that probe too far into people's lives (i.e., aspects that may not affect one's ability to do the job reliably). Others argue that the administration of such tests is based on the assumption (sometimes false) that corporations have the ability, above and beyond the applicants themselves, to decide which job is best for whom.

Biometrics-

Biometric authentication refers to those technologies that are capable of analysing human biological and other characteristics for identification purposes. Examples include fingerprinting, eye-scanning, and body measurements and the idea behind such measurements is that they, unlike other forms of personal information, are hard to copy or steal. To date, biometrics has not been utilized on a grand scale for workplace purposes, but because of increasingly effective and inexpensive technology, this is likely to eventually change (the market for biometrics grew from $500 million in 2002 to $4 billion in 2007, and continued growth at this rate is anticipated).

The use of biometrics presents privacy concerns because of (a) the fact that biometric information, by its nature, involves the personal characteristics of people who may not want to share in the first place especially to a government or other agency that may abuse that information in



the future, and (b) biometric information could be as potentially susceptible to identity theft as other kinds of identification methods.

Drug Testing-

Drug testing is increasing in the work place because most current illicit drug users are employed and drug use by these employees can influence performance and even their safety and the safety of those around them. Because the National Institute on Drug Abuse reports that these employed drug abusers cost their employers twice as much in medical and worker compensation claims as their drug-free co-workers, employers are highly motivated to prevent their employees from using illicit drugs. Common purposes for testing include pre-employment testing, random testing, reasonable suspicion testing, post-accident or incident testing, and treatment follow-up testing. Types of drug tests commonly required by employers include urine, hair, sweat, and saliva drug screens.

Because drug tests can be intrusive and even embarrassing (urine tests are sometimes conducted while medical personnel observe), a chief concern is that drug tests are too invasive and intruding for the benefit they provide. (Some studies, including the 1994 National Academy of Sciences and the 2004 Independent Inquiry into Drug Testing, have not been able to link drug use other than alcohol with workplace health and safety risks.)

Genetic Testing-

Although few employers currently use genetic testing, because of the rapid growth of this science, it's anticipated that this will change in the near future-especially because the benefits could arguably be to both employees and employers. Genetic testing is the analysis of genes, chromosomes, and proteins in order to predict risk of disease, identify disease carriers, diagnose disease, or determine the likely course of a disease. Genetic testing can be used, for example, to detect genetic abnormalities resulting from workplace exposure to toxins or to detect susceptibility to workplace toxins. Currently, about 900 types of tests can detect about 50 different disorders that impact peoples' susceptibility to certain workplace toxins.

Genetic testing has obvious potential to aid both employers and employees, but the privacy question arises once again exactly how much information should an employer have about a particular employee? Should employees have to merely hope that their employers will not opportunistically or negligently abuse their personal information?

Wi-Fi and Public Access Computing:

Wi-Fi and Public Access Computing refer to the technology that has allowed people to access the Internet in shared locations. Anyone with a Wi-Fi-enabled device such as a computer or a handheld cell phone can connect to the Internet when he or she is near an access point, which covers a certain geographical area ranging from a few square feet to several city blocks. Wi-Fi technology is now often used by people and companies for Internet and phone access, though the technology is expanding to include many kinds

of electronic devices.

The benefits of convenience provided by Wi-Fi are obvious, but there are also some potential privacy risks. Specifically, operators of "access points" are often able to access, if they so desire, the computers of those using their access points. This can also work the other way as well people can hijack access points to gain services that they have not paid for, and they can even damage the access points or computers connected to them. As a result, privacy is at risk.

Information Privacy:

The fact that H-P was using pretexting to gather the personal phone records of its board members was insufficient to trigger information privacy concerns. That is, one must have knowledge that his or her personal information is vulnerable to outside control, that is, no longer under his or her sole personal control.

When Dunn received a report from the spying she had ordered, she called a meeting of the board. There she announced that board member George Key worth was the source of the leaks. Key worth was dismissed from the board, but another board member, Thomas Perkins, who objected to the methods used, also resigned from the board, and it was not until September of 2006 that the controversial use of pretexting was made public. H-P was required to report to the SEC of board changes. This, coupled with pressure from Perkins, led to the September 2006 disclosure from H-P of the pretexting effort. A firestorm of criticism and scrutiny ensued, and the very public nature of H-P's spy activity made salient the risk that organizational members faced.

Conclusion:

Information privacy continues to be a concern as organizations increasingly collect and handle employee personal information. Presumably, the ultimate goal of these efforts is to ensure competitive viability and survival of the organization. At the same time, these efforts can have theparadoxical effect of actually making organizations less competitive, particularly if information privacy is not maintained. For example, and as discussed, information privacy is inextricably linked to intrinsic motivation, and employees whose privacy is threatened will be less motivated to share knowledge, take risks, and provide the types of creative input that will ensure an organization remains competitive.

With respect to H-P, the verdict is still out. In January 2007, then Attorney General Lockyer offered to reduce the felony charges to misdemeanours in a plea arrangement. Dunn and the others accused refused to cop a plea- presumably because they could have still been under jeopardy at the federal level. In March of 2007, however, the new attorney general Jerry Brown dropped all charges against Dunn and the others. Thus, even in a state like California, where workplace privacy is given more credence, it is often difficult to prosecute organizations for spying activities that threaten employee privacy, as the H-P case illustrates. It remains to be seen whether federal charges will be brought against the participants in the H-P pretexting case.

References :-

1. Aiello, J. R. (1995). Electronic performance monitoring and social context: Impact on productivity and stress. Journal of Applied Psychology, 80(6), 738-745.
2. Alder, G. S. (2001). Employee reactions to electronic performance monitoring: A consequence of organizational culture. Journal of High Technology Management Research, 12(2), 323-342.
3. Alge, B. J. (2001). Effects of computer surveillance on perceptions of privacy and procedural justice. Journal of Applied Psychology, 86(4), 797-804.
4. Alge, B. J., Ballinger, G. A., Tangirala, S., & Oakley, J. L. (2006). Information privacy in organizations: Empowering creative and extra-role performance. Journal of Applied Psychology, 91(1), 221-232.
5. Alge, B. J., Greenberg, J., &Brinsfield, C. (2006). An identity-based model of organizational monitoring: Integrating information privacy and organizational justice. In J. Martocchio (Ed.), Research in personnel and human resource management, (Vol.25, 71-135). San Diego, CA: Elsevier.
6. Altman, I. (1975). The environment and social behavior: Privacy, personal space, territory, crowding. Monterey, CA: Brooks/ Cole Publishing.
7. Amabile, T. M. (1983). The social psychology of creativity: A componential conceptualization. Journal of Personality and Social Psychology, 45(2), 357-377.
8. Amabile, T. M. (1988). From individual creativity to organizational innovation. In K. Gronhaug& G Kaufmann, G (Eds.), Innovation: A cross-disciplinary perspective (pp. 139-166). New York: Oxford.
9. Amabile, T. M. (1997). Motivating creativity in organizations: On doing what you love and loving what you do. California Management Review, 40(1), 39-58.
10. American Management Association. (2005). Electronic monitoring and surveillance survey. New York: Author.
11. American Management Association. (2007). American Management Association (AMA) management training and professional development seminars, workshops and books. Retrieved September 2, 2007, from http://www.amanet.org/
12. Bernstein, J. (1999, April 22). Financial identity theft. Federal Trade Commission. Retrieved September 3, 2007 from http://www.ftc.gov/os/1999/04/identitythefttestimony.htm

Dr. Anil Chidrawar
I/C Principal
A.V. Education Society's
Degloor College, Degloor Dist.Nanded