# Psychological Effects of Workplace Surveillance on Employees, and the Legal Protection: An Analysis

**Dr. Vidushi Jaswal***

## Introduction

David Lyon says: "Surveillance is the monitoring of the behavior, activities, or other changing information, usually of people for the purpose of influencing, managing, directing, or protecting them."[1]

Surveillance provides the surveillor the requisite amount of information about its subjects for fulfilling its intended purposes. The employers subject their employees to surveillance for enhancing their profits. It means that private organizations conduct surveillance over its employees for some economic reasons. The employee's surveillance is being done to prevent theft and sabotage, increasing productivity, preventing lawsuits, avoiding violent incidents in the workplace, and preventing terrorist attacks.[2] One of another economic reason is to prevent the non-work related use of company resources.

Furthermore, the employers do not want to be held liable for their employee's behavior. Therefore, the employers spy on employee's improper use of web resources which ranges from copyright infringement (e.g., downloading and installing copyrighted software) to sexual harassment issues associated with web pages containing pornographic content, and inappropriate e-mail that promote a hostile work environment.[3] Although the right of the employer to conduct workplace surveillance is permissible under the law, it should be done in a fair and reasonable manner.[4]

---

* Assistant Professor, MCM DAV College, Chandigarh.

1 David Lyon, *Surveillance Studies: An Overview* (2007). First published, Polity, Cambridge.

2 Frederick S. Lane, *The Naked Employee: how technology is compromising workplace privacy*, 12 (2003).

3 R.J. Boncella, *Internet Privacy: At Home and At Work*, Communications of AIS, Volume 7 Article 14, 1-28, at 12. *Available at* http://www.washburn.edu/faculty/boncella/INTERNET-PRIVACY.pdf accessed on April 29, 2013, at 5:52 p.m. IST.

4 Lucas D. Introna, *Workplace Surveillance, Privacy and Distributive Justice*, Computers and Society, December 2000, 33-39, at 34. *Available at* https://cb7088bd-a-62cb3a1a-s-sites.googlegroups.com/site/lucasintrona/home/journal-publications/publication-archive-1-1/WorkplaceSurveillance%2CPrivacyComputersandSociety.pdf?attachauth=ANoY7cr5BiiSc3eRjapp3KsTK7PTbiQzPijtdVAVZufFPcy3A8faoBsuggcwiSjDAvKb

In recent times, while using sophisticated surveillance techniques like DNA profiling, hidden cameras, global positioning system (GPS) devices, etc., the employers have increased the workplace surveillance without even bothering its effects on their employees. Due to unhealthy completion in the business world, the employees' private or personal life has also become the subject matter of workplace monitoring. All this happens because the employer and the employee are never on the equal positions. The employer always holds the dominated position in case of bargaining with the employee.

## Psychological effects of workplace surveillance in the contemporary world

Excessive surveillance at workplaces have negative effects on employees such as increased stress, loss of identity and the emergence of privacy issues. In many surveys, it has been observed that the employees who are under surveillance are more likely to suffer from health, stress and moral problems. In many cases, the workers fail to take pressure under surveillance conditions and quit the job.[5]

Alan Westin says: "If surveillance does not provide necessary space to a person for his actions and thoughts, he would face certain schizophrenic implications".[6] Indeed, privacy is definitely required for the effective operation of social structure.[7] Only those who can sustain an absolute commitment to the ideal of perfection can survive total surveillance. However, this is not the condition of men in ordinary society.[8]

Furthermore, an individual has right to disclose secrets about his soul or personality to whom he likes. But compulsion to reveal

---

cUkJuexi5Ovx-HXrbEyfYDPFRCqEicP52nFe7G3S-h95PVSbCyySlvJ0JjXMoPbdkaWqlfA1OVHLzTEkiVNyWNFuOu8xrj4iube3l5bBz917Q0NQ0PRm2YW-7nvil4CNP23BchNdaCx4Qfak8dCgzC4P2js328o9gWB3suDVZ3OaLu4XtCov6gutuRwDIwrdT4N9drcHdj8BYjibZjNs2E5YC7EWdS-n5zGgjNhSnj4xTaCtnGi9Tesj2MVgcQzQkA8v4eJYEWt5TetVQUi8OJISmG77WQ%3D%3D&attredirects=0, accessed on June 17, 2012, at 1:00 pm IST.

5 Jane Ragoo & Reeaz Chuttoo, *The Negative Effects of CCTV Workplace Surveillance*, LeMauricien.com. *Available at* http://www.lemauricien.com/article/negative-effects-cctv-workplace-surveillance, accessed on January 20, 2017.

6 Alan F. Westin, *Privacy and Freedom*, 57 (1970).

7 *Id.* at 58.

8 *Id.* at 59.

those parts of his memory and personality that he regards as private, amounts to violation of person's psychological privacy.[9]

Unreasonable and arbitrary workplace surveillance violates the employees' right to privacy. If the employees fail to enjoy their privacy at work, they feel suffocated and depressed. Here, privacy means both informational and decisional. Privacy enables control over personal information as well as control over our bodies and personal choices for our concept of self.[10]

Violating an individual's privacy affects the development of his personality and identity. It also affects his personal autonomy. In such circumstances where an employee is under continuous surveillance, he or she may not be able to develop meaningful relationships with others. Apart from the effect that a lack of privacy can have on the individual, it can create aggregated problems on the level of society. Democracies require an autonomous and open individual who is willing to engage with others. A lack of privacy can mitigate against the development of these individuals as well as their willingness to engage with others. And then one of the economic arguments is that missing employee privacy can hurt labour relations.[11]

In recent times, the employers act in the capacity of communication providers when they provide sophisticated equipment to their employees. By using such equipment, the employees access cyberspace. In exchange for providing that access, employers collect every personal detail of their employees. With the help of various software and network management tools, the employers read employees' e-mail and track employees' every cyber activity.[12] Many employers usually ask very personal questions before and during employment. They install miniature hidden cameras in the offices to prevent crime by, and to improve efficiency among their employees.[13]

Furthermore, it has been seen that the employers are always anxious to know the results of their employees' DNA sample. DNA

---

9 *Id.*at 61.

10 Joseph Kupfer, *Privacy, Autonomy, and Self-Concept*, American Philosophical Quarterly, Vol. 24, No. 1 (Jan., 1987), 81-89 at 87. *Available at http://www.jstor.org/stable/20014176,* accessed on August 24, 2011, at 8:48 p.m. IST.

11 Bernd Carsten Stahl, *Ethical Issues of Information and Business*, *in* Kenneth E. Himma and Herman T. Tavani (eds.), THE HANDBOOK OF INFORMATION AND COMPUTER ETHICS 311-335 (2008) at 321.

12 Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193-1294 (1998) at 1233.

13 Malcom Warner and Michael Stone, *The Data Bank Society*, 68 (1970).

sample may provide the information about an employee's future efficiency level, which is of great concern for the employers. Thus, by using DNA report the employers may draft the contract of service as per according to their own wishes. Such contract of service may result to be discriminatory in nature. If DNA report discloses an employee's future incurable disease or any other disease which could affect his services, then the employer would make contract for limited period only. After utilizing the employee's energy, the employer may terminate his services, hence, would be violative of one's fundamental right to livelihood. Therefore, the developments in Human Genome Research, and its use by employers, and insurance companies have increased the danger of violation of an individual privacy.

Genetic testing can be defined as any technique that can be used to gain information about aspects of an individual that are influenced, caused by, or controlled by genes. In health care, genetic testing is used to identify predispositions to rare genetic diseases (e.g., Huntington's disease), to predict response to drugs, to estimate risks for developing common illnesses (e.g., some cancers), and to determine carrier status for reproductive purposes.[14]

Genomic information serves public good by identifying and understanding etiology and pathophysiology of disease. With the help of Genetic testing, medicine and science have expanded the abilities to prevent and ameliorate human malady. However, such Genetic information can be used to invade a person's private lives, and family life.[15]

Genomic data has the capacity to identify an individual and his family members, and can make present and future health profiles with more scientific accuracy than any other health data. Therefore, any breach of such informational privacy results into economic harms, such as loss of employment, insurance, or housing. Ultimately, it results into social stigmatization, embarrassment, loss of self-esteem, and much more psychological harm. Although genomic information cannot be fully trusted, public perception aggravates the stigma and discrimination.[16]

At workplaces, the employers are easily accessing the clinical records of employees. By doing such testing, they can determine

---

**14** Patricia A. Roche, "Genetic information and testing", in William G. Staples (ed.), *Encyclopedia of Privacy*, (2007), 252-256, at 252.

**15** Lawrence O. Gostin, "Genetic Privacy", 23 *J.L. Med. & Ethics*, (1995), 320-330, at 320.

**16** *Id.*at 324.

an employee's current and future capacity to perform a job**.** Such records can also be used for pension and health care benefit plans. Despite the existence of legal restrictions under disability discrimination, such testing is still in practice.[17]

Moreover, the use of Radio Frequency Identification (RFID) equipped with GPS technology at the workplaces has also increased the privacy concern. RFID is a generic term used to describe technologies that involve the use of data stored on small chips or tags which can be communicated to a reader from a distance by means of radio transmission.[18] It means that the huge amount of people's personal information can be stored on a small chip. Moreover, such information can be read from distance. Initially, the RFID devices were being used to prevent shop lifting. However, these technologies are now being used at the workplaces to monitor the employees. For the purpose of monitoring, the employers may compel their employees to wear RFID small devices on their uniforms, wrists, fingers or arms.

Jennifer Stoddart, Privacy Commissioner of Canada, said that the 'workplace privacy' is a significant part of one's personal autonomy. If the employees do not enjoy privacy at work places, then it would have bad impact on employees' sense of dignity, their sense of freedom, and their sense of autonomy. The Commissioner said that the continual surveillance is a very dehumanizing process. Obviously, it affects the enthusiastic workforce.[19]

Cameras increase stress, anxiety and reduce productivity. Workers are frightened to take breaks and have an increased risk of repetitive strain injuries. One case has occurred where a boss constantly flashed a message to a lowly easily and heavily monitored data processor: "You are working less hard than the person next to you". This increased anxiety and lowered productivity.[20]

---

17 *Id.*at 321.

18 Office of the Privacy Commissioner of Canada, "Radio Frequency Identification (RFID) in the Workplace: Recommendations for Good Practices", 1-36 (March 2008). *Available at* http://www.priv.gc.ca/information/pub/rfid_e.pdf, accessed on June 16, 2012, at 2:00 pm IST.

19 Address by Jennifer Stoddart, Privacy Commissioner of Canada, "Finding the right workplace privacy balance," The Ryerson University Workshop on Workplace Privacy, November 30, 2006. *Available at* http://www.privcom.gc.ca/speech/2006/sp-d_061130_e.asp. accessed on June 18, 2012, at 2:20 pm IST.

20 Adrian Furnham, *The Psychology of Surveillance*, PSYCHOLOGY TODAY. *Available at* https://www.psychologytoday.com/blog/sideways-

Therefore, employees do expect privacy at work places, even if the place belongs to their employer. Obviously, employers need basic information about their employees for many lawful things. However, the collection of information through illegal means, and without the consent or knowledge, is the violation of employees' privacy.

**Legal protection to the employees against the workplace surveillance**

The Fourth Amendment of the United States' Constitution guarantees the freedom from unreasonable searches and seizures. However, by showing some probable cause, the law enforcement agencies can get the search warrants from the courts of law. Therefore, the Fourth Amendment generally restricts physical intrusions upon employees' privacy interests, such as the right to be free from the searches caused by employer drug testing, medical and genetic testing, employer searches of the person and property of employees, and employer surveillance and monitoring of employee activities and communications.

The constitutional right to privacy also prohibits the employer's intrusions into the employee's personal decisions. However, the courts allow the search and seizures of a government employee on the grounds of "special governmental needs". Similarly, the courts in Unite States justify public-sector drug testing programs for the safety of public or employee. But the courts do not allow such drug testing programs in case of less compelling circumstances.[21]

Increasingly, the federal Employee Polygraph Protection Act of 1988 limits the ability of private sector employers to conduct polygraph examinations and other lie detection tests of employees and job applicants. In general, pre-employment polygraph testing is allowed of job applicants in very limited circumstances, specifically when employers are involved in providing security services or in manufacturing or distributing controlled substances. Private employers can conduct polygraph examinations only in connection with an ongoing investigation of economic loss or injury to the employer and then only of employees with access to the property at issue and for whom there is reasonable suspicion of involvement in the loss or

view/201507/the-psychology-surveillance, accessed on January 12, 2017, at 5:20 pm IST.

21 L. Camille He'bert, "Workplace Privacy", in William G. Staples (ed.), *Encyclopedia of Privacy*, (2007), 615-620, at 616.

injury.[22] In case of lie detector test, the employer is subject to the following restrictions:

- The employer cannot ask questions about employee's religious beliefs, sexual preference, racial matters, lawful activities of labor organizations, and political affiliation.
- The employee has the right to refuse to take a lie detector test.
- The employer must explain how the test results will be used.
- The employee has the right to stop the test at any time.
- The employee can request that questions not be asked in a "degrading and needlessly intrusive fashion."[23]

Another federal legislation that regulates the employers' action of surveillance is the Omnibus Crime Control and Safe Streets Act of 1968, as amended by the Electronic Communication Privacy Act of 1986. This Act, also known as Wiretap Act, places restrictions on the ability of employers to intentionally intercept or attempt to intercept oral, wire or electronic communications of employees.

In India, privacy has been discussed mostly in terms of the protection of the individuals' rights against the government's unreasonable search and seizure. The courts in India have recognized that the right to privacy is a part of fundamental right to life and personal liberty. While accessing the constitutionally inherent powers of the higher judiciary in India, both public and private employees can enforce their right to privacy against the unlawful surveillance.

For example, in *People's Union for Civil Liberties v. Union of India*[24], the Supreme Court held that wiretapping invades an individual's privacy. The Supreme Court held that the telephone tapping by Government under S. 5(2) of Telegraph Act, 1885 amounts infraction of Article 21 of the Constitution of India. The court said that the right cannot be curtailed "except according to procedure established by law," which should be just, fair and reasonable.

Government employees also enjoy privacy protection under the Right to Information Act, 2005. Except in case of public interest, the government employees' personal information cannot be given

---

22 *Id.* at 617.

23 Frederick S. Lane, *The Naked Employee: how technology is compromising workplace privacy*, 274 (2003).

24 (1997) 1 S.C.C. 301.

to anyone. Sections 8(1)(a) to 8(1)(j) of the Right to Information Act, 2005 contain a list of categories of information which are exempted from any kind of disclosure. However, under Section 8(2),[25] all these exemptions can be waived if a public authority decides that public interest in disclosure outweighs the harm to the protected interests.

In *G.R. Rawal v. Director General of Income Tax (Investigation)*[26], the Commission (CIC) said that Section 8(1)(j) excludes from disclosure an information which relates to personal information, the disclosure of which

- has no relationship to any public activity or interest; or
- would cause unwarranted invasion of the privacy of the individual.

Personal information also means sensitive personal information. According to Section 2 of the UK Data Protection Act, Sensitive Personal Data means personal data consisting of information as to:

- the racial or ethnic origin of the data subject
- his political opinions
- his religious beliefs or other beliefs of a similar nature
- whether he is a member of a Trade Union
- his physical or mental health or condition
- his sexual life
- the commission or alleged commission by him of any offence
- any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

Therefore, such 'sensitive personal information' of government employees cannot be disclosed to anyone.

---

**25** Section 8(2) of the Right to Information Act, 2005 provides as follows:
Notwithstanding anything in the Official Secrets Act, 1923 (19 of 1923 ) nor any of the exemptions permissible in accordance with sub-section (1), a public authority may allow access to information, if public interest in disclosure outweighs the harm to the protected interests.

**26** Appeal No. CIC/AT/A/2007/00490. *Available* at http://www.rti.india.gov.in/cic_decisions/Decision_05032008_01.pdf, accessed on May 31, 2013 at 12:00 p.m. IST.

In the case of *Neera Mathur v. LIC*[27], LIC Corporation asked its employee Neera Mathur to disclose the information about her menstrual cycles, conceptions and pregnancies and abortions. But the Supreme Court of India ordered the Corporation to delete such questions because such information is embarrassing and humiliating, and pertains to one's personal autonomy.

Furthermore, the Information Technology Act of 2000 empowers the employees in India to protect their personal information from their employers' access. The Information Technology (Amendment) Act 2008 has made the provision of civil liability in case of computer database theft, computer trespass, unauthorized digital copying, downloading and extraction of data, privacy violation etc. Section 43A of the Information Technology Act provides for 'compensation for failure to protect data'. It is provided that negligent act on the part of a body corporate in relation to protection of sensitive information, which causes wrongful loss or wrongful gain to any person, is subjected to pay compensation to that person.

After the Amendment, the range of cyber offences has been widened and, sections 65--74 include offences related to unauthorized tampering with computer source documents,[28] dishonestly or fraudulently doing any act referred to in section 43,[29] sending offensive messages through communication service etc.,[30] dishonestly receiving stolen computer resource or communication device,[31] identity theft,[32] cheating by personation by using computer resource,[33] violation of privacy,[34] cyber terrorism,[35] transmitting obscene material in electronic form,[36] etc.

Section 66E of the Information Technology Act punishes electronic voyeurism. It provides the punishment for violation of privacy. It punishes those who intentionally or knowingly captures, publishes or transmits the image of private area of a person. This

---

27 A.I.R. 1992 S.C. 392.
28 The Information Technology (Amendment) Act 2008, s. 65.
29 *Id.* s. 66.
30 *Id.* s. 66A.
31 *Id.* s. 66B.
32 *Id.* s. 66C.
33 *Id.* s. 66D.
34 *Id.* s. 66E.
35 *Id.* s. 66F.
36 *Id.* s. 67.

offence is punishable with imprisonment of up to three years or with a fine of up to Rs. two lakh or both.[37]

The Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 define the term 'sensitive personal data and information' (SPDI) and prescribe 'reasonable security practices and procedures' (RSPP). Under the said rules, the employers are required to adopt the reasonable security practices and procedures and sensitive personal data or information rules.

In one of the decision the Madras High Court directed the employers to remove the CCTV cameras from the employees' rest room. The court in *Raptakos Brett Employee's Union v. The Deputy Commissioner of Labour, DMS Compound, Teynampet, Chennai*[38] said that the employer and employees should maintain a smooth cordial relationship for the welfare of all concerned.

## Conclusion and suggestions

In India, the existing data protection legislations are not sufficient to tackle the ongoing excessive workplace surveillance. The privacy laws need to be tuned with the labor jurisprudence. Following things are yet to be done for protecting the employees from psychological effects of surveillance:

- Workplace monitoring should be reasonable, transparent, accountable and proportional.

---

37 The Information Technology (Amendment) Act 2008, s. 66E.

**66E.** Punishment for violation of privacy.- Whoever, intentionally or knowingly captures, publishes or transmits the image of a private area of any person without his or her consent, under circumstances violating the privacy of that person, shall be punished with imprisonment which may extend to three years or with fine not exceeding two lakh rupees, or with both. Explanation - For the purposes of this section—

**(a)** "transmit" means to electronically send a visual image with the intent that it be viewed by a person or persons;

**(b)** "capture", with respect to an image, means to videotape, photograph, film or record by any means;

**(c)** "private area" means the naked or undergarment clad genitals, pubic area, buttocks or female breast;

**(d)** "publishes" means reproduction in the printed or electronic form and making it available for public;

**(e)** "under circumstances violating privacy" means circumstances in which a person can have a reasonable expectation that—

**(i)** he or she could disrobe in privacy, without being concerned that an image of his private area was being captured; or

**(ii)** any part of his or her private area would not be visible to the public, regardless of whether that person is in a public or private place.

38 W.P.No.29883 of 2013, decided on 1-12-12014, Madras HC.

- The informed consent of the employees is required.
- The employees' information should be protected from unauthorized accesses.
- Employee's medical information should be kept secret and confidential. It should not be misused.
- Drug testing and DNA testing of employees need to be regulated.
- The employees should be provided with appropriate remedies having deterrent effect, against the employers' arbitrary surveillance.
- CCTV cameras at workplace should only be installed after assessing the appropriate risks.