

Blurred Work - Life Frontiers: A Paradigm Shift in Employee Social Networking Privacy

Vikas Trivedi^{1*} and Vaishali Trivedi²

¹Institute of Law – Nirma University, Ahmedabad, Gujarat, India; vikastrivedi99@rediffmail.com

²St. Kabir Institute of Professional Studies, Ahmedabad, Gujarat, India; drvaishali@skips.in

Abstract

A large number of millennials are expected to join the workforce by the year 2020. The 'Selfie Generation' as they call it, differs from the previous generations in terms of their workplace attitudes, aspirations and technological adaptations. They exhibit great affinity to digital world. These characteristics of millennials are going to have a strong impact on the future workplaces. Growing popularity of digital gadgets and social media among the millennial workforce has become a cause of concern among corporate. Digital craze among employees may make them sometimes blind to the dangers of sharing sensitive information about their employers/ organizations which may result into troubles for the firms in question. Modern day employers have started monitoring their employees conduct (including monitoring the employee's social media accounts, mobile communications, laptops etc) at and beyond official work frontiers, to their defense. But as there are always two sides to a story, this form of monitoring has put employee privacy at risk, thereby blurring their personal-professional (life) boundaries. This paper seeks to study the contemporary trends in employee monitoring and resulting issues concerning employee social networking privacy. The paper also seeks to address the ethical and legal dimensions connected with employee social networking privacy.

Keywords: Digital Craze, Employee Monitoring, Millennial, Social Networking Privacy, Work Frontiers

Paper Code (DOI): 20925; **Originality Test Ratio:** 1%; **Submission Online:** 16-Apr-2018; **Manuscript Accepted:** 20-Apr-2018; **Originality Check:** 23-Apr-2018; **Peer Reviewers Comment:** 30-Apr-2018; **Double Blind Reviewers Comment:** 02-May-2018; **Author Revert:** 13-May-2018; **Camera-Ready-Copy:** 20-May-2018; **Editorial Board Excerpt:** 30-May-2018.

Editorial Board Excerpt: *At the Time of Submission (ToS) submitted paper had a 01% plagiarism which is a good indication as far as originality report is concerned and fall under an accepted percentage for publication. The editorial board is of an observation that paper had a subsequent surveillance by the blind reviewer's which had been rectified and amended by an author in a range of phases as and when required to do so. The reviewer's had in an initial stages comment with minor revision with a following remark which at a short span restructured by an author. The comments related to references, abstract and body text is noticeable both subject-wise and research wise by the reviewers during evaluation and further at blind review process too. All the comments had been collective at a variety of dates by the authors' (vikas & vaishali) in due course of time and same had been integrated by the author in addition. By and large all the editorial and reviewer's comments had been incorporated in a paper at the end and further the paper had been earmarked and decided under "Theme Based Paper" category as its highlights and emphasize the work in relation to Employee Social Networking Privacy*

1. Growing Internet Penetration and Eruption Digital of Volcano

India is on the verge of becoming the youngest country in the world by the year 2020 signifying the role the millennials are expected to play in its growth. Millennials are also said to be the torch bearers of India's Digital revolution. According to report titled India@Digital Bharat the number of internet users are expected to grow to over 550 million by the year 2018. Currently India is the second largest country in terms of mobile internet users in the world.

It is predicted that business landscape and in turn the world of work would be greatly influenced by the millennials, a cohort born between 1980-2000 who are entering the workforce in huge numbers. Currently India has over 400 million millennial representing one third of its population consisting 46% of its workforce. A loyalty-lite, techno freak generation that prefers to communicate electronically, increasingly hooked to social tools like social networking, apps, blogs etc. A research by COMPTIA suggests that one of the key trend governing future workplaces will be blurred lines between individual's personal and professional lives due to extensive use of technology by the millennials.

Thus sharing of the information via social networking sites by the socially active employees is increasingly becoming a cause of concern for the corporate as also acknowledged by the employees? This has resulted in adoption of various practices pertaining to monitoring the social media indulgence of the employee, by the modern day employers.

With social media surveillance of employees taking the front seats in the corporate, employees are getting increasingly concerned about the invasion of their privacy by their employers.

This paper attempts to examine the contemporary trends in employee monitoring and corresponding issues concerning employee social networking privacy. The paper also seeks to address the ethical and legal dimensions connected with employee social networking privacy.

2. Managing the Impressions

The underlying psychology of growing millennial craze for social media can be well understood through *Erving Goffman's* theory of self presentation (1959) which suggests that it is the mass media context that impacts the interpersonal interactions amongst the millennials. Millennials are able to create vivid versions of them while communicating with the world through various social media platforms. They are found to be more reserved during face to face conversations but are more comfortable while communicating through social media as it provides them an opportunity to draft the message in advance.

Furthermore, Millennials have a drive to succeed and expanded drive related to accomplishing career objectives¹⁸. This parallels how Millennials utilize social media and outlines their reliance on gathering of people cooperation when utilizing social media. If at all, by chance millennials fail to get responses on their posts, they may alter them or erase the content as to not diminish social rank or ubiquity. Myers and Sadaghiani (2010)⁹ suggested that millennials feel comfortable communicating their considerations and suppositions with others and are comfortable addressing specialist figures through social platforms. Seemingly, narcissism can be seen in how Millennials utilize social media, particularly Facebook.

Narcissistic inclinations rise on social media as millennials have an overstated capacity to control their image by posting what they regard as imperative or commendable¹⁰. This can be accomplished by posting status overhauls portraying a life occasion they had fairly taken part in, posting a picture of a fantastic involvement, or sharing another Facebook user's post about an encounter they shared. This is an illustration of how impression is being created on social media.

Millennials utilize social media for excitement, instruction, and most imperatively, as source of interpersonal communication². This gives the era, communication alternatives that their

forerunners didn't have accessible. Many a time's millennials have been able to make connections with people from distinctive nations as social media provides them with easy and prompt access. Moreover, the era is able free from virtual circumstances or discussions millennials find unappealing, with more ease and less repercussions than one might encounter with in-person discourses. The negative suggestions/comments on social media on millennials strengthen their resolve to modify their self presentation. By modifying the ways they show themselves on virtual platforms, millennials make an image of self that is alluring to world outside. All said and done, every time the use of social media is not negative in nature. Social media is seen to have boosted person's self-worth or self-esteem.

Millennials utilize social media for various purposes this utilization may take several forms, such as a individual venting disappointment in a status toward companions and family or posts in community groups depending upon common interests³. Individual is able to feel a sense of approval through the number of likes or comments gotten on a post. Millennials were found to utilize social media for individual acknowledgment and as approval from connections with people in their contacts.

3. Progressively Blurred Work-Life Frontiers

In this age of digital revolution, it is difficult to ascertain whether an employee is busy with the organizational work or personal business at any given juncture. Employees these days retrieve employer's computer systems from home both amid and beyond standard working hours. Employees frequently interact with one another by email at all hours from any place. They also regularly utilize employer owned computers both within and outside the conventional work environment to engage with social media. Moreover employees often bring their private electronic gadgets to work for the personal use as well as for the company work. Employees increasingly install social apps like Facebook, Whatsapp, Instagram not only on their personal gadgets but also on company's gadgets to get in touch with external world.

4. Objective of the Study

1. To explore the recent trends in employee monitoring,
2. To analyse the reasons for employee surveillance,
3. To analyse the concerns of employee privacy with respect to social media usage, and
4. To examine the ethical and legal aspects related to employee monitoring in Indian context.

5. Employee Monitoring or Invasion of Employee Privacy

From the theories of Taylor to McGregor and Elton Mayo, it can be inferred that there is a consistent need on the part of employers to figure out how to oversee humans at work. There is a continuous need to manage and motivate employees at work. Though times have changed but one thing has remained consistent. Employers always want to be ensured that everybody is doing the work at the pace and carrying out the work as per the expressed standard. Technological advancements come to the aid of employers in the pursuit of this endeavor thereby making them monitor the employees electronically. But sometimes this monitoring leads to emergence of issues concerning employee privacy majorly related to data privacy and surveillance. Employee monitoring takes two basic forms - Covert surveillance means intentionally monitoring employees in confidential way ie without them being aware of the same. Secret monitoring is very not easy for a manager to legitimize, and must only be utilized in extraordinary circumstances.

Overt observation happens when managers surveil workforce, with the employees informed of this act.

5.1 “Why” of Employee Monitoring

Employers have logical thought processes for electronically monitoring their employees' conduct, as they are exposed to various risks like:

1. *Leakage of Confidential or Other Non-Public Information:* Through discussion boards or while networking with professionals such disclosure can include:
 - Highly confidential information that damages the organization's competitive status,
 - Product or other related information that may contradict with the organization's official communications, and
 - Organisation's proprietary information or trade secrets.
2. *Hazard to Company Computer Systems, Network or Data:* Utilizing an organization's PC, or cell phone to engage in online networking, with dangers of introducing conceivable pernicious programming or other harmful applications, particularly for web-based social networking that includes downloading malicious files.
3. *Inappropriate use of company's resources:*
 - Using a company computer or smart-phone to engage in social media, leading to excessive speed utilization or visiting improper websites etc.,
 - Without consent using the company title, symbol, trademarks, copyrighted data or other intellectual property in

- blogs or other social networking platforms that can encroach on the company's rights to and control over these assets, and
- Engaging in social networking through corporate email account which indicates his employment relationship with the company.

4. *Inappropriate use of work time:* To discourage non-work related web activities during work hours
5. Investigate and anticipate the illegal unfair badgering of individual employees.
6. To get hold of electronic conversations or records may be the subject matter of creating legal liabilities or corporate record keeping policies.
7. Protecting client data and other important information from being leaked.

5.2 Employee Monitoring Strategies

Employers these days use various techniques to keep a close eye on the employees. Technological advancements have made their jobs easy. The most common strategies by which employers conduct employee surveillance:

Direct observation: Sometimes employers hire people to oversee the employees at work without them having knowledge about them same.

Telephone tapping: Recording the telephone conversations on office phones is one of the most common methods employed by employers to keep a watch on the employees.

Computer: Computer programs like screen recording software's are increasingly used by the employers that provide them with an access to employees' computer screens, hard drives and screen keystrokes to assess efficiency. Through keystroke monitoring, employers can see the details of every key pressed by the employee on a particular day.

Mobile: Conversations made by employees on smart phones, laptops etc provided by the employers can be monitored by the employers. As these gadgets are owned by the employer, it's legally permissible in most of the cases.

Email monitoring: Employers monitor conversations made through company's official email account and sometimes private emails too if they are made through company's computer.

Video surveillance: CCTV cameras are installed by the employer within the office premises that capture the video recordings of various activities in which employee indulges into during his/her working hours.

Geolocation: Employers increasingly use GPS technology to detect the location of the employees through installing devices in the company owned vehicles.

Photo copying machine and fax memory is reviewed by the employer to find out which type of documents is photocopied by the employees.

5.3 Rise of Wearbles

With the proliferation of technology, more and more companies are urging their employees to use wearable gadgets in the name of employee wellness initiatives. In 2013, as many as 2,000 firms across the globe offered their workforce fitness trackers. This number rose to around 10,000 by 2014 seeing the rising trend thereafter. According to some analysts by the end of year 2018, as many as 2 million employees will be mandated to put on health-and-fitness trackers as a part of their service contract.

The use of wearable gadgets raises privacy concerns for the employees as these gadgets record the personal data of an individual which may be used by the employer for monitoring the employees digitally even after the working hours. For example, the employer can easily track employees' location and heart beat even after work hours which can be truly irritating to an employee. Moreover, there is a potential risk of employees' personal and sensitive data getting hacked as it is store at multiple destinations ie with employer or third parties.

5.4 Corporate Insights

With the rapid technological breakthroughs corporate are able to monitor almost all the activities of their employees. A Swedish startup Epicenter embeds microchips in its employees' bodies that works as swipe cards for them for various tasks like open entryways, work with printers, or purchase snacks by simply waving the hands. A tracking gadget named "OccupEye" has been introduced by British multinational bank to oversee how often employees are at their work stations.

Amazon monitors its employees utilizing GPS tags while they are inside the warehouse. If at all by chance, any employee is found to be breaking any of the organization's rules, for example, conversing with fellow mates or early departure from work, he could be fired if the frequency of breaking the rules goes beyond established limits.

Deloitte uses a device called 'Humanize' employee badge that examines employees' tone of voice, speed with which he moves, intensity of his interaction with others, sleeping behavior etc.

6. Next Wave of Monitoring – Social Networking Sites

6.1 Social Media Landscape

To effectively appraise the implications of social media for corporate it's vital to understand its various uses. As indicated by Wikipedia, web-based social networking is extensively used for:

- Correspondence, for example, micro-blogging, web journals, blogs, and occasions,
- Collaborated efforts, as wikis, social news and bookmarking/tagging,

- Sight and sound, including video, photography, music/sound sharing and introduction sharing and live casting, and
- Amusement, for instance, media stages, virtual universes and diversion sharing.

Social media plays an important role these days in hiring decisions, creating strong employer brand and to communicating with clients. As per a survey by CareerBuilder (2016), as many as 70% of the employers were reported using social media for screening of the candidates. The fact that as many as 54% employers accepted to have not hired the candidates on the basis of content posted by them on social media shows the importance that modern day employers attach to the digital footprints of the candidates. 47% of the small to midsized business organizations planned to extend their employer brand using social media as per estimates of LinkedIn Survey 2016, highlighting the growing preference of social media amongst corporate for hiring purposes. Last but not the least; companies are increasingly leveraging social platforms to make a variety of communications with their clients through press releases, promoting other stuff, for handling client complaints etc.

The popularity of social media is not only restricted to the employers but the employees also use social media extensively for a variety of tasks. Utilizing online networking has a prompt impact as larger audience in general can be made aware about a situation or event quickly after it has emerged or occurred. This can prompt undesirable reputation and consequences for a business when such post is directly related to an organization.

Employers may screen employees' activities on social media platforms by asking them to share their usernames and passwords for their personal accounts. A few companies have social media policy that permits them to take employees to task for posting certain data/ content on social media platforms.

According to the survey by CareerBuilder (2016), 28% of the employers surveyed have accepted to have reprimanded or fired their employees for engaging in activities like checking Whatsapp or Facebook, online shopping etc during work hours. 18% of the employers have accepted to have pink-slipped their employees for posting inappropriate content on social media.

As per the findings of 2014 global survey, by Proskauer as many as 70% of the employers reported to have penalized the employees for misusing social media. The survey further highlighted that organizations are increasingly taking precautions to secure themselves against particular hazards connected with abuse of social media, For example-

- Abuse from claiming secret data (80%),
- Misrepresentation of the facts and figures of the company (71%),
- Belittling comments about the company or its staff (64%), and
- Badgering (64%).

7. Eternal Ethical Dilemma: Should Employee have the Right to Privacy?

As the trend for social media monitoring by employers is gaining momentum, employees and groups advocating privacy are raising their concerns about ethical dimensions of invasion of employee privacy.

Ethical frameworks can by and large be divided into two types: deontological and teleological morals. As indicated¹⁶ consequentialists (teleological) are moral scholars who advocated that an action can be said to be morally right only by judging its consequence. If the outcomes are great, that act is right else not.

Going by this theory, Social media surveillance of employees private accounts by the employer can be said to be morally correct as such surveillance will help them to achieve good results for the business i.e. keeping the company's reputation and integrity safe and intact.

However, analysing the same from the employee's perspective, the outcome of such surveillance may not be always great for the employees. As already discussed that individuals use social media for expressing themselves freely which also includes expression of dissatisfaction, venting out anger and frustration sometimes against the employers as well, this kind of monitoring can potentially invite a disciplinary action against them.

Deontology is referred to as obligation based ethics. It suggests that actions are more important than consequences. It evaluates the motives or intentions behind any act. It preaches about continually acting in good faith and stays committed to the Golden Rule i.e. to treat others the way you need to be treated by others.

7.1 According to the Famous Law of Karma (Action) Stated in Bhagavad Gita, all the Actions must be Performed without any Attachment to the Consequences

Going by this theory, social media surveillance of employees private social accounts by the employer can be said to be morally correct since it is employer's duty to observe the practices which are in the best interest of the business irrespective of its good or bad consequences on the employees.

However the same act can be seen as ethically wrong from the perspective of employee as this act of invading the privacy of an individual means restricting their basic human right of freedom of expression. This very act is seen as unethical irrespective of the consequences it may have for the employees or the organization.

8. Legal Dimensions of Employee Privacy

There is no denial to the fact that employees increasingly access social media inside and outside the workplace. On the other hand, employers concern regarding the social media usage by the employees also seems genuine. Generally the employer can view the content posted by the employee on social media which is visible to public. However there are certain state laws which limit the employer's ability to have a close eye on the employee's social media activity. In UK, Federal Stored Communications Act restricts the employers to access employee's non public Facebook posts without employee's authorization.

Also laws in various states restrict the right of the employer to ask for the username and password of employee's private social media accounts. In some countries like New Mexico, law prohibits the employer from requesting an employee for extending various social media considerations like – adding the employer to the contact or friend list on social platforms; requiring employee to change the privacy settings of his account so that employer can have an open access to the content being posted; asking for any information that would help them access employee's private social media account.

Indian constitution does not have any provision relating right to privacy explicitly however right to privacy has been considered as subset of fundamental right to life and personal liberty by honorable Supreme Court of India under Article 21. Also the scope of exercising this right has been restricted to any government action. Violations of such rights by any non government body may be tried with under the principles of torts.

The only law that has endeavored to address the issue of data security under Indian Constitution is The Information Technology Act, 2000 ('IT Act'). Sensitive Personal Data on Information (SPDI) is safeguarded under Section 43(A) and personal information is protected from illegal revelation in breach of contract under Section 72A of the act. The act directs the entities engaged in collecting, storing or dealing with SPDI to comply with certain rules as laid down under this act. .

8.1 Compliances Related to SPDI

Different parameters and compliances have been laid down under IT Act for the employers to follow while handling employee Sensitive personal data.

- The act calls for collecting SPDI only in case there is a requirement to collect such data for legal and indispensable purposes,
- Specific written approval (which also includes consent via electronic modes) must be obtained from the employees pre-

ceding collection of the SPDI. The workforce must be made aware of necessity of the collection of sensitive personal data, about the parties who would have access to this data and also the specific details of the items of SPDI being collected. They must also be informed about the fact if the data would be further transferred to any other parties,

- Employees must also be provided with an opt-out option,
- IT Act directs employer to have a well-documented privacy policy that must also be displayed on company's website,
- The employees must be allowed retrieve the information and be permitted to amend and make necessary updating in the information,
- As per the provisions of the act, the company can retain employee's sensitive personal information only up to the time its lawfully required,
- Employee's permission must be obtained prior to disclosing his SPDI to anyone, and
- The employers must establish adequate security procedures to ensure protection of SPDI.

The act clearly states that failure or negligence on the part of the employer to comply with any provisions of the act would make employee entitled to receive compensation from him.

9. The Way Ahead

It is clear that with the benefits associated with utilizing social media in the working environment there is a potential risk that may invite employee lawsuit and a bunch of other legal issues. Since the social media is used universally and represents a trend not likely to fade away in near future, it is judicious for employers to be apprised of and get ready for these potential risks. A few recommendations for managers to dodge these dangers include:

- Companies must design a clear cut social media policy stating what all is allowed and what all isn't allowed. Directives in policies should neither be overly vague nor too restrictive. Considering the complexity of legal matters it is suggested to avail the services of legal experts while formulating such policies.
- Generally companies may disallow the revelation or utilization of confidential information, exchange of insider facts and client information, but such restrictions must be tailor-made so as to disallow the revelation of proprietary information and the managers must be able to illustrate that they have taken steps to protect the privacy of such critically sensitive information.
- Employees must be educated and made aware about the possible disciplinary actions in case of any misuse of social media by them.

- Employees must be clearly communicated that employer has the right to screen their communications made through the company's computer and communication frameworks. Also they must be strictly advised to not to use personal gadgets for accessing social media during the working hours.
- For any articulations or comments posted on social platforms that is either in the organisation's name or could sensibly be credited to the company, the employees may be asked to state expressly that they are not posted on behalf of the company except in case of promotion of company's products or services.
- Managers must be trained for managing such social media issues which may emerge on the part of employees as also the issues pertaining to employees' social media privacy.
- The employees must be informed at the time of leaving the organization that use of company's computer network and its data is disallowed.
- Company-issued tablets, smart-phones, laptops etc. must be taken back by the managers well in time from the employees who are leaving and reviewed to assess whether certain company data has been misused.
- All the employees must be asked to give in writing that they do not expect any privacy with respect to any information that is exchanged through company owned computers and other communication frameworks.
- The companies must continuously update their social media policy in compliance with current laws.

To conclude, 'millennial social media addiction' is the trend that is here to stay for long. With more millennials joining the workforce, the corporate are under constant threat to be on the receiving end of the negative consequences of their employee posting sensitive information on social platforms. The notion of privacy is fast changing. The intrusions that were unacceptable in the past have now started gaining acceptance within employee fraternity. The line between acceptable and unacceptable intrusion is getting hazy swiftly.

Given the pace of technological advancements it is feared that in the name of safeguarding company's security and employee efficiency, the employers may justify tracking employee brainwaves and other biometric measures in the time to come.

Collecting extremely sensitive information like passwords by employers is wrong on moral grounds too and can lead to restricting the right to freedom of expression.

On the legal side, despite the regulations is decently in nascent stage in India, employee social networking privacy concerns would assume center stage in the years to come. Thus it is necessary for the employers to estimate the gravity of these concerns and prepare themselves to comply with the new legislations and at the same time protecting their own interests. Enactment of right to privacy (Privacy Bill) has already been initiated by

the government. Time will tell whether the Privacy Bill goes through. Meanwhile employers ought to prepare themselves for compliance with the rules. Law makers and the corporate must see to it that in the wake of protecting intellectual property of the companies individual's basic right to freedom must not get destroyed.

10. References

1. Brignall III TW, Van Valey T. The impact of internet communications on social interaction, *Sociological Spectrum*. 2005; 25(3):335-48. <https://doi.org/10.1080/02732170590925882>.
2. Callegher J. The costs of bonding: Negotiating personal information disclosure among Millennials and Boomers on Facebook; 2013.
3. Myers KK, Sadaghiani K. Millennials in the workplace: A communication perspective on millennials' organizational relationships and performance, *Journal of Business and Psychology*. 2010; 25(2):225-38. <https://doi.org/10.1007/s10869-010-9172-7>. PMID: 20502509 PMCID:PMC2868990.
4. McCain JL, Campbell WK. Narcissism and Social Media Use: A Meta-Analytic Review, *Psychology of Popular Media Culture*. 2016. <http://dx.doi.org/10.1037/ppm0000137>.
5. Pfeil U, Arjan R, Zaphiris P. Age differences in online social networking—A study of user profiles and the social capital divide among teenagers and older users in MySpace, *Computers in Human Behavior*. 2009; 25(3):643-54. <https://doi.org/10.1016/j.chb.2008.08.015>.
6. Shaw W, Barry V, Sansbury G. *Moral Issues in Business* (1st Asia-Pacific ed.), Cengage Learning, Melbourne, Australia; 2009.
7. Skues, J., Williams, B., Oldmeadow, J., & Wise, L. (2016). The effects of boredom, loneliness, and distress tolerance on problem internet use among university students. *International Journal of Mental Health and Addiction*, 14(2), 167-180.
8. White K, MacDonnell R, Dahl DW. It's the mind-set that matters: The role of construal level and message framing in influencing consumer efficacy and conservation behaviors, *Journal of Marketing Research*. 2011; 48(3):472-85. <https://doi.org/10.1509/jmkr.48.3.472>.

Annexure-I

Blurred Work - Life Frontiers: A Paradigm Shift in Employee Social Networking Privacy

ORIGINALITY REPORT

1%

SIMILARITY INDEX

PRIMARY SOURCES

1	www.skips.in Internet	20 words — < 1%
2	www.nishithdesai.com Internet	16 words — < 1%

3	www.nirmauni.ac.in Internet	10 words — < 1%
4	worldwidejournals.in Internet	8 words — < 1%
5	Soo-Jin Lee, Sandra, and Emily Borgelt. "Protecting Posted Genes: Social Networking and the Limits of GINA", <i>The American Journal of Bioethics</i> , 2014. Crossref	8 words — < 1%

EXCLUDE QUOTES ON EXCLUDE BIBLIOGRAPHY ON EXCLUDE MATCHES OFF

Source: <http://www.ithenticate.com/>

Prevent Plagiarism in Publication

The Editorial Board had used the ithenticate plagiarism [<http://www.ithenticate.com>] tool to check the originality and further affixed the similarity index which is 01% in this case (See *Annexure-I*). Thus the reviewers and editors are of view to discover it suitable to publish in this *Volume-10, Issue-1, January-March, 2018*.

Citation:

Vikas Trivedi and Vaishali Trivedi

"Blurred Work - Life Frontiers: A Paradigm Shift in Employee Social Networking Privacy", *Global Journal of Enterprise Information System*. Volume-10, Issue-1, January-March, 2018. (<http://informaticsjournals.com/index.php/gjeis>)

DOI: 10.18311/gjeis/2018/20925

Conflict of Interest:

Author of a Paper had no conflict neither financially nor academically.