Ethical and Legal Consequences of Corporate Online Social Networks (OSN) Sites in Pakistan

Erum Naz Akhtar[1], Dr. Tahir Hameed Ullah Khan[2], Ayesha Abbas[3], Tayyiba Kausar[4],

Iram Rehman[5], Sijal Mehmood[6]

[1]*Manager*, Department of Law, Capital University of Science & Technology (CUST), Islamabad, Pakistan, erum.naz@cust.edu.pk

[2]*Professor*, Department of Law, Capital University of Science & Technology (CUST), Islamabad, Pakistan, tahir@cust.edu.pk

[3]*Lecturer*, Department of Management Sciences, International Islamic University (IIU), Islamabad Pakistan, ayesha.phdmgt148@iiu.edu.pk

[4]*Lecturer*, Department of Management Sciences, International Islamic University (IIU), Islamabad Pakistan, tayyiba.phdmgt184@student.iiu.edu.pk

[5]*PhD Scholar*, Department of Management Sciences, International Islamic University (IIU), Islamabad Pakistan, Iram.phdmgt195@student.iiu.edu.pk

[6]*MS*, Human Resource Management, Capital University of Science & Technology (CUST), Islamabad, Pakistan, sijal24@yahoo.com

***Correspounding Author: *Naila Rafique**
Assistant Professor Law, Capital University of Science & Technology (CUST), Islamabad, naila.rafique@cust.edu.pk

Abstract

Corporate social networking offers a great opportunity for employers and employees to connect and exchange work-related information. Unfortunately, using online social networking (OSN) sites is not specifically covered by the laws of the Islamic Republic of Pakistan. Future social networking rules will be modeled by the National Labor Relations Act of the Islamic Republic of Pakistan, as a civil rights legislation act, and common law principles like employment at-will and defamation. Besides security, efficiency, correctness, and justice in discipline, the forthcoming legislation is also impacted by ethical factors including kindness, privacy, etc. Employers and employees of interests should be stable in corporate social networking policy. Social media platforms are having a negative impact on Pakistani youth, and many people in the country misuse OSN. Although laws exist, Pakistan continues to face the possibility of restrictive measures against OSN sites and the internet. Laws now in effect and ethical concerns surrounding social networking should influence social networking rules, including formation, communication, correction, and policy review. Corporate social networking rules ought to be focused on business, guarantee user notification of monitoring, keep sufficient

International Journal of Stress Management
2025, Vol. 32, No. 1, 1-17

documentation, and offer a loyal, uniform, and objective assessment of the efficacy of monitoring.

Keywords: Corporate social network (OSN) sites, Law, ethics, administrative policies.

INTRODUCTION

Businesses are finding new ways to connect with customers online and disseminate information among employees of organizations and customers/clients, etc., and promote goods and services through online social networking (OSN) sites such as LinkedIn, Instagram, Facebook and many others. There are 200 million people using Facebook in April 2009 (McCarthy, 2009). In contrast to others 22.4% reach, 29.9% of the world's internet users are on Facebook, and it is the most lucrative social network, with almost 1 billion US$ in 2008 income compared to 300 million US$ for Facebook. Except Japan, Germany, and Brazil, Facebook dominates the social media landscape worldwide (Ostrow, 2009). The growth rate of Facebook since February 2008 has been 228 percent. In just over a year, the number of unique visitors to x (formerly Twitter), a platform where users may publish microblogs of up to 140 characters in length, climbed to 7 million (Sutter, 2009). Instagram, launched in October 2010 by Kevin Systrom and Mike Krieger, rapidly gained popularity with one million listed users in just two months, in one year 10 million, and by June 2018 1 billion users were recorded. With 2.4 billion active users as of right now, Instagram accounts for almost one-fourth of all active internet users worldwide. There are now around 13.91 million Instagram users according to “State of digital” in Pakistan in 2022.

Regardless of organizational structure, corporate social networking sites are gaining popularity for a number of reasons, including branding, discovering, exposing, and utilizing intellectual capital that is hidden; increasing workers enthusiasm and gratification; and creating goods and services more quickly (Communitelligence.com, 2009). Finding individuals and information, considerate associations, creating common values, enhancing customer relationships, improving knowledge management, retaining younger workers who are much aware of OSN sites, and also keeping former workers in the loop are all things that this software can help businesses with (CIO Insight, 2009).

This paper's original contribution lies in its proposal of management policies for business engagement with social networking sites by integrating the ethical and legal aspects of such sites. For proper use of these emerging technologies, social networking studies are required to go in light of the ever- changing ethical and legal landscape of these platforms.

LEGAL ISSUES

Historically, employment laws have been applied to both employers and workers' usage of OSN sites like Facebook, Instagram, and LinkedIn. There are no legal regulations of the usage of these OSN sites from the start till now, despite the fact that several observers have voiced the opinion that such regulations should be put in place (Byrnside, 2008). Some cybersecurity laws are proposed, but they are not very popular for practice where these laws are highly required for the safety of OSN users. Courts still use old common law and current federal and local legislation to decide employment matters using OSN sites, even though lawmakers of the Islamic Republic of Pakistan are still trying to figure out how to handle this and other new kinds of communication technologies. An employer-maintained OSN page might lead to an embarrassment of legal complications. Even though most workers are considered to be employed at-will, there are certain situations where an employee's engagement with their employer's OSN page could reveal information about their membership in an officially protected class, engage in legally protected activities like labor organizing or whistle-blowing, or involve other forms of concerted action. In addition, if an employee violates company policy by posting sexually explicit content or other sensitive information on the company's official social media profile, the employer might be held vicariously liable. Employees also have the right to reveal information that the law mandates their employers keep hidden, such as specific employee information, trade secrets, or important details about a future securities transaction. The employer may be held criminally liable if an employee were to submit illegitimate information. Companies can protect themselves against this kind of lawsuit by revising their existing internet policy to spell out in detail how workers are expected to behave when using the company's OSN page.

EXCEPTIONS TO THE EMPLOYMENT AT-WILL POLICY

In most cases, the employment-at-will theory governs employment matters, which implies that employees typically resigned or terminated for any cause or for no reason at all (Grubman, 2008). Therefore, it is often permissible to terminate an employee's employment if any of them is engaged in inappropriate behavior on the employer's OSN site, whether it's during working hours or not. It is unclear whether an employer-maintained OSN site would give rise to a claimable case against the employer; despite this, there are a few common statutes and legislative exceptions to employment at will that may be pertinent to any legal issues that arise in this situation.

A Silent Agreement to Act Honestly and With Good Faith. Employers could face legal consequences for their "bad faith" actions concerning the circumstances

and terms of employment in the small number of jurisdictions that acknowledge this exception to the employment-at-will doctrine (Lichtenstein and Darrow, 2006; Sprague, 2007). It is considered "bad faith" and a violation of the indirect agreement of good faith and fair dealing when a company offers a reward to a worker, such as retirement benefits or sick leave, and then dismisses or demotes them for utilizing those benefits (Grubman 2008 and Gutman 2003). This means that employers who have policies in place regarding OSN run the risk of legal action if certain employees are treated differently than others, for example, if an employee is told their social media activity is fine but then gets in trouble for it or the employer tries to get out of paying them promised benefits because of it (Grubman, 2008; Sprague, 2007).

Contract, Whether Explicit or Implicit. Several courts have ruled out that an employment relationship is not at-will if the manager enters into an explicit or implicit agreement with the employee (Gely and Bierman, 2006). A company may face legal consequences if they violate their contractual agreement on fair cause terminations. For example, if an employee is dismissed for publishing anything on the business's OSN site that isn't really linked to their work or isn't sufficiently incorrect, the employer might be held accountable.

The Right to Whistle-Blow About Public Policy. The public policy exemption to employment- at-will might apply in a wide range of circumstances. If firing an employee would violate the state's official public policy, it is considered an unfair dismissal (Grubman 2008 and Gutman 2003). If an employee is dismissed for showing up to board service, for instance, there might be a case of unfair termination because it is a statutory obligation that all citizens are required to fulfill according to state legislation.

Similarly, when an employee refuses to violate the law on behalf of their company or exercises a fundamental right, the public policy exception is typically available (Grubman, 2008; Lichtenstein and Darrow, 2006). If a company allows its employees to be active on its OSN page, then this might be considered as an indicator of the fact that the company is allowing them to talk about their job and their connection with the company. An employee may be protected from legal action if they disclose information about their employer's OSN page in a remark or other post.

Legislation at the federal and state levels encompassed under the public policy exemption protects workers who "blow the whistle" on their employers' unlawful actions from revenge. As an example, retribution against an employee who "has opposed any practice made an unlawful employment practice" by the 1964 Civil Rights Act (1964) is explicitly forbidden under Section 704 of Title VII of the Act. Similar provisions may be found in other federal acts, including:

- Sarbanes-Oxley Act of 2002 (On July 30 of that year, the U.S. Congress passed a law to assist shield investors from corporate financial reporting deception).

- Family and Medical Leave Act of 1993 (To provide temporary medical leave and family leave in specific situations).
- Professional Safety and Health Act of 1970 (To provide safe and healthy working conditions for both men and women in the workforce by permitting the application of the Act's requirements).
- Fair Labor Standards Act of 1949 (The Act only establishes a minimum salary beyond which neither employer-employee negotiations nor changes in the economy may compel wages. It stipulates that workers falling under its purview must receive a state-set minimum wage (Kirkland, 2006; see also Clineburg and Hall, 2005).

In order for an employee to be protected by state whistleblowing rules, the person must have correctly reported the alleged infractions to the relevant government agency (Kirkland 2006).

However, without other measures, an employee's remarks made on an OSN site may not normally protect them from the employer's ensuing reprisal.

DISCRIMINATION LAWS AND SEXUAL HARASSMENT EMPLOYER LIABILITY

If an employee claims that his/her employer discriminated (e.g., for disclosing a protected status online), the applicable statutes may be federal or state law. Consider a hypothetical situation where a supervisor invites other employees to his social and religious services; this may happen if the company’s employer permits its employees to utilize the business Facebook page for personal messages. If other employees file a complaint, is the employer required to remove the post? But in order to fulfill its duty to appropriately accommodate an employee's religious views or practices, does the employer have to permit the job to remain in place? If workers post information about their protected characteristics (race, color, religion, gender, and national origin) on their workplace's OSN, they may be protected under Title VII of the 1964 Civil Rights Act (Rubman 2008). Among other state and federal laws, the Age Discrimination in Employment Act (1967) and the Right Person with Disabilities Act (2090) prohibit discrimination in the workplace on the basis of protected traits, convictions, and/or actions.

Vicarious Liability Issues

When employees commit torts while acting in the course of their employment, employers are typically held vicariously accountable, according to respondent superior (Greenbaum and Zoller, 2006). There are several options for employers who are running their official business OSN sites to take on this kind

of responsibility for user-generated content. The site's content might be slanderous, infringe on the privacy of employees or others, or, in extreme cases, cause emotional anguish. They may even insinuate illegal activity, for which the company may face legal consequences.

Public shaming. Precautions should be taken by employers to ensure that their official OSN site is not liable for any defamatory postings made by employees or others. Defamatory content posted by an employer on their own website might potentially lead to legal action (Lex, 2007). However, does this protection extend to comments published on the company's OSN site by friends or staff members?

Consider the following hypothetical situation: An employee publishes a fake statement on the company website, claiming that Mr. A worked today till late hours to use the company's printer for printing his daughter's college assignments and notes. Given that the employer is in charge of the website and decides who can access it, might they be found vicariously liable to Mr. A if this comment meets the basic defamation standard, which is an inaccurate and harmful statement transmitted to at least one other person?

According to a number of authorities, if an employee posts defamatory remarks on their employer's blog while acting in the course of their employment, the employer is often liable under the respondent superior approach (Grubman 2008 and Gutman 2003). The subject of whether or not an employee's involvement with an employer's OSN page qualifies as work-related activity is an intriguing one. Employer-maintained OSN sites and workplace blogs are very similar. In either scenario, who has access to the site and what they can publish are up to the group managing it. On the majority of OSN sites, you can typically remove user comments as well. An employer may be held accountable in a tort lawsuit if they fail to exercise sufficient control over their employees or if their negligence permits the activity to continue (Gutman 2003).

However, due to the informal nature of OSN sites, multiple posts on a company page may not constitute defamation (Lex 2007). The site is primarily used for communication rather than hard news or research; many potentially defamatory statements can escape liability because users do not necessarily perceive what they read as reality (Lex2007). On the other hand, it implies that users can get the impression that they can say whatever they want in such a casual setting without worrying about consequences from the law. No matter how casual the comment, if it satisfies the defamation requirements, the speaker may be held legally accountable (Lex2007). Only a few cases could pose a serious threat to the judicial system as it currently exists, given that over 100 million people use it. Anyone accessing an employer-managed OSN page is likely to assume that the material is acceptable to the organization, especially in such circumstances.

Another issue is the accountability of individuals who repost defamatory remarks. If someone reposts a false statement, they are typically just as

accountable for defamation as the original publication (Lex, 2007). This ruling might not, however, apply to an employer's obligation for posts on their OSN site that are defamatory and made by a friend or employee. Providers and users of interactive computer services were exempt from liability for posting certain information, including potentially defamatory content, when Congress added the "Good Samaritan" clause to the Communications Decency Act of 1996 in 2000 (Benedict, 2009; Lex, 2007). The Citizens Protection Against Online Harm Regulations 2020, which are governed by the 2016 Prevention of Electronic Crimes Act and the 1996 Pakistan Telecommunication Act, social media platforms like Facebook, Google, Instagram, and X (Formerly Twitter) are obliged to block or remove posts deemed objectionable. Information that the federal government can demand ranges from personal information to traffic and content data. In addition, online platforms will have to remove any content that the government deems “unlawful” within 24 hours and in special emergency cases in under six hours. This rule states that no one who provides or utilizes an interactive computer service may be considered the speaker or author of any content that has been supplied by another trustworthy source. However, the wording of the Act and later legal interpretations may lead to such protection for individuals, even if it seems that Congress may not have meant for the Good Samaritan clause to apply to individual OSN users (Lex, 2007). Applying this exemption clause to individual online social network users is difficult because Congress approved this provision prior to the development of more modern technology such as online social networks.

Whether an organization can be held liable for posts made on its official OSN page by friends or employees that are defamatory depends on how much the business participates in the republication of content. If you think (Lex 2007) is right: The degree to which an organization is complicit in the republication of content determines whether it may be held accountable for defamatory posts made by employees or friends on the organization's official social network page. If you believe (Lex 2007): The likelihood that an OSN user will be recognized by the courts as the original publisher increases with the user's involvement in the dissemination of the item. The most evident situation where an OSN user could be protected is if someone else makes derogatory comments in the user's "Comments" area. In this instance, the user would have passively replicated the claims, in the same way that AOL (formerly America Online) and CompuServe reproduce forum posts from the start of internet times till now. In Pakistan this law protects the social media plateforms as they are not responsible, as described: No provider or user of an interactive computer service shall be treated as the publisher. Bloggers are not liable for comments left by readers. But, websites, blogs, and social networks that host speech with protection against a range of laws that might otherwise hold them legally responsible for what their users say and do.

Even though employers might not be held accountable for libelous allegations, they should exercise caution when it comes to who they approve of as friends and closely monitor any comments or activity on the official OSN page. Allegations pertaining to privacy violations in the workplace typically fall into one of three categories: confession of personal information to the public, interference with privacy or seclusion, or deceptive public representation of an individual (Gabel and Mansfield 2003). Public exposure is the most frequent of the three possible outcomes that might occur when an employee shares personal information on the organization's social media accounts, or OSN. A breach of privacy occurs if the employee has a legitimate expectation of secrecy with regard to the material in question (Brandenburg, 2008). Courts have almost always determined that employees do not have a legitimate expectation of privacy regarding a variety of online communication methods, such as computer Internet access and work email systems. (Milligan, 2009). However, those situations typically include employees who voluntarily transmit their data.

If a worker reasonably expects confidentiality concerning the material in question, then there is a violation of privacy (Brandenburg, 2008). When it comes to a variety of online communication methods, such as computer Internet access and corporate email systems, courts have almost always rejected the idea that employees do not have a legitimate expectation of privacy (Milligan, 2009). On the other hand, those instances usually include workers who voluntarily send their data.

- Do these holdings apply to posts made by other users on an OSN website that the company runs?
- Undoubtedly, if a company purposefully posts private employee information on its public Facebook profile, it might be subject to immediate legal action for breach of privacy.
- What happens then if a colleague or friend of the employer posts offensive content to the business website? Because of such, may the employer also be held accountable in a vicarious capacity?

Employers may be held vicariously liable for any damages if their official social media account (OSN) is sufficiently associated with their place of employment and if they are aware of the offensive post but fail to remove it right away.

Sprague (2007) and Gabel and Mansfield (2003) state that proof of willful, outrageous behavior is required for justifications of action based on the purposeful infliction of emotional distress. When an employee files a claim for such an injury, it is their responsibility to demonstrate that the employer's actions, whether they take the form of putting comments directly on the employer's OSN or keeping another user's post there, were unreasonable and resulted in severe mental distress for the worker.

Consider the following circumstances: A link to explicit content is posted by an employee on the company's OSN website. A former worker with some grievances threatens his boss with murder on the business' official social media page. If anything similar happened, may the business be subject to legal repercussions?

Business should take legal action, as according to a general rule, employers are liable for their employees' illegal behavior as long as the activities are directly related to the employment relationship (AmJur 2d 2009). Using company property for illegal purposes is another factor that could result in criminal charges for the employer (Gutman, 2003).

Confidential Information Disclosure, Trade Secret Theft, and Securities Fraud: When performing business as an employee, employers risk liability if they reveal confidential information, including personnel data, on their OSN page or even on the employee's personal page (Grubman, 2008; see also Gutman, 2003). If workers reveal their employer's trade secrets to the public, they risk legal repercussions from both their employers and state or federal trade secret statutes (Clineberg and Hall 2005 and Grubman 2008). Furthermore, Section 10b-5 of the 1934 Securities and Exchange Act prohibits the disclosure of significant, nonpublic information in certain circumstances. If the employer posts such information on the company's networking site, they may be in violation of the 10b-5 rule, especially if the company's stock price is fluctuating (Clineberg and Hall, 2005; Grubman, 2008).

If an employer posts such information on the company's networking site, they may be in violation of the 10b-5 rule that created corporate liability beyond registration statements, allowing investors to sue for any misleading statements or omissions, especially if the company's stock price is fluctuating (Clineberg and Hall, 2005; Grubman, 2008).

Legal and Ethical Issues: Legal and ethical norms are different, even though they often overlap and have different functions. Laws have a key objective: to maintain the stability of social institutions. It is their responsibility to decide if social sanctions against particular individuals and their behavior are justified. Ethics is the study of right and wrong behavior, mainly concerning itself with the advancement of social concepts rather than in enacting laws. A person's own personal code of behavior is another possible description of ethical principles (Candilis, 2002). It is quite permissible to disregard the guidelines provided by many professional codes of ethics. For example, it is not illegal for a professional doctor to act disrespectfully toward others. According to Sims (2003), the legal system is not broad enough to meet society's expectations about how its members ought to act in ethical dilemmas. The ethical perspective offers an extra lens through which to look at appropriate social media activity. Concerns about social networks and those regarding the internet, email, and routine office tasks could involve some overlap in effort.

In addition to fair data collection, which is a direct cause of many social media problems like privacy, accuracy, and security, we address issues of discipline and dignity. Productivity, discipline, and dignity are different from issues associated with the equitable gathering of information because of their relative emphasis on superior business practices, procedural fairness, and the state of being respected and esteemed.

Legal and Ethical Concerns: If a boss is using the company OSN site to write private notes, the risk of sexual harassment and the disclosure of sensitive information to superiors are both heightened by the degree to which one's private and public lives intersect (Greenbaum, 2008, Schultz, 2008). Corporate OSN sites provide an opportunity for employees to connect, but when users indulge in idle discussion about matters unrelated to work, it may soon become an unhealthy fixation. Business social networks are expensive and inefficient. In 35% of commercial social network activity, there are fewer than 100 members (Kirkpatrick 2008). Less than 25% of those companies have more than a thousand subscribers, despite the fact that more than half of them have invested more than multi-million rupees on the websites. The primary problems with corporate networking sites have been excessive, ostentatious features; poor social network management; and ignorance of the authenticity of the information obtained from such sites.

Monitoring content on a business's OSN site to prevent inappropriate networking may take a lot of time and resources (CIO Insight, 2009). It's possible that a monitor won't be able to differentiate private information from professional. In the event that an employee has committed any misconduct, a monitor might reveal personal information about them. Supervisors have the right to partially accuse an employee of misconduct without carrying out a detailed inquiry, even if the claimed misbehavior has nothing to do with their job. A monitor may target a person or group by investigating a non-random selection of workers. Furthermore, a monitor might look at a sample right before the launch of the designer’s work, when it's easiest to provide personal information.

The potential for workers to expose sensitive information about the business, including passwords, new offerings, and services, on a company intranet website is a security issue. Social media users may accidentally or on purpose reveal private information about a company, such as its financials, marketing strategies, business plan, or future products and services. 10% of businesses investigated the possibility of financial data being leaked through internet forums, according to a study that was based on interviews with 300 IT decision-makers (Warnock 2007). Should there be a confidentiality breach, secret firm information could end up in the public domain. If a company's secrets are kept secret from the public, they may be subject to hacking (Kaupins and Minch, 2006). Private Data: There are numerous ways that a worker's privacy could be violated. Pictures uploaded online might be used to show off to coworkers at stressful events like

family gatherings. Making disparaging statements about friends, family, and other relatives might lead to jealousy and misuse of photos. If you write on people's walls a lot, they can get irritated and block you and other comments. Potentially inflammatory topics include religion, politics, sexism, and racism (Urban Dictionary, 2008).

Employers may easily find out information about their staff members with the help of specialist spy webs, Google, and other search engines. For example, Spokeo can import full e-mail address books of persons, just like its competitors People and CV Gadget. They can find out if someone has updated their internet activities by keeping an eye on their contacts (Raphael, 2009).

The social network's ability to change its terms of service at any time further erodes privacy. Words like "We reserve the right, at our sole discretion, to change, modify, add, or delete portions of the Terms of Use at any time without further notice" can have a big influence on privacy policies.

Employers should not browse potential employees' social media profiles to learn about personal information such as race, health, political inclinations, or religious views. This is especially unethical when the posts are made during the job search process. An employee's personal social media accounts should never be viewed by a firm (Greenbaum, 2008).

Management may not be aware of the authenticity of posts made on a company social media account. An employee may cause damage to the company’s image even by briefly posting false financial information on a social networking platform and then removing it. It could be challenging to prove that an employee made any potentially harmful posts if they remove them. According to the Ethics Scoreboard (2009), individuals who share deceptive content on social sites can be playing a practical joke on their viewers. Owing to the restricted screen area, factual data might be shown separately. Users can hide additional messages by clicking the "click here for more posts" button (Schultz 2008).

Rejecting friend invitations received through corporate OSN platforms by employees may leave volunteers and coworkers with hurt feelings. According to Coyote Communications (2008), volunteers and staff should respect people's wishes to keep their OSN activities separate from their professional relationships.

A respectful approach is when someone is esteemed, honorable, or worthy; they possess dignity. If their bosses find out or disseminate negative, inaccurate information about them, workers might be less inclined to value one another (Kaupins and Minch, 2006).

Certain OSN platforms are illicit to employees of certain government bodies and businesses. On a number of these platforms, the use of assistive technology, people with certain disabilities, and users of out-of-date hardware and software encounter additional difficulties. This suggests that since many individuals cannot access OSN platforms, organizations should not focus their outreach efforts only on them. Examples of these platforms include blogging, instant messaging, and

photo sharing, e.g., Instagram, WhatsApp, snapchat, etc. Therefore, it is not recommended

To make your OSN outreach the only emphasis of online outreach activities in order to avoid missing out on a significant number of people (Coyote Communications, 2008; Bondfield, 2008).

Suggestions for Organizational Policies

Existing legal and ethical concerns may have a big impact on organizational social networking strategies. The employer's wish to operate a profitable business must be balanced with the employee's Right to Privacy. A legal monitoring policy would typically cover a wide range of topics, such as how monitoring is set up, communicated and punished, and its overall effectiveness assessed. The range of each dimension might be anything from very active to no action at all. These four dimensions are based on the work of Kaupins and Minch (2006). Configuration surrounds OSNs as the operating shell. Characteristics that are addressed include who will be observed, how they will be observed, and when and where the observation will take place. It acts as the operating shell and encases OSNs. "Communication" means informing staff about the OSN regulations. Informing staff members of the where, when, and how secure policy communication will be is crucial.

The three primary facets of discipline are corrective, progressive, and the hot stove rule. Progressive discipline focuses on giving workers heavier penalties for more serious infractions. The employer may use a written warning if an employee's inappropriate behavior doesn't change after being given verbal warnings. Suspension or termination are examples of additional disciplinary measures. It is imperative to provide the employee with advice on appropriate behavior on social media sites as a form of corrective discipline. Following the therapy session, the client's networking activities may be properly observed in the future. The hot stove rule states that all kinds of discipline must be prompt, uniform, impersonal, and preceded with a warning. Discipline must always be applied in a way that is appropriate for the gravity of the offense and the type of business.

When it comes to evaluation, every monitoring rule should be examined for its validity, dependability, and potential drawbacks for employees. We must gather data regarding people's activities on social media. It is imperative that all monitoring policies undergo periodic assessments and updates. The policy endorsements based on the four previously mentioned factors are compiled in Table 1. Every dimension includes a list of significant policy concerns. The answers are based on recommendations from experts in the fields of developing codes of ethics, legislation, international organizations, government rules, and

employee handbooks. When faced with questions like "Who will do the monitoring?", businesses are offered various possibilities.

Table 1. Recommendations for OSN sites Management

Dimension	Subjects	Sample Solutions
Formation	Verification schemes	Using devices or password-based user authentication methods (Owyang, 2008)
Configuration	Monitoring people	IT executives, administrators, and upper management (Department of National Affairs, 2009)
Configuration	Technology used	Company's computer system (Bersin, 2007)
Configuration	People observed	For business purposes alone, data is aggregated equally across every people (American Civil Liberties Union, 2008; Nolan, 2004).
Configuration	Period of monitoring	During working hours (All Business, 2001)
Configuration	Place of monitoring	• Office inspection should be the only monitoring directed (Hartman, 1998; National Work Rights Institute, 2004). • Keep an eye on what matters (James, 2004).
Configuration	Behavior acceptable	• Make sure you understand the goals of the societal encounter, for instance, making valuable associates (Warnock, 2007). • Don't talk about private commercial ventures. Avoid personal communication and just provide business-related information. Don't make disparaging remarks. Urban Dictionary, 2008; Warnock, 2007)
Configuration	Strategies coordinated	Combine entirely automated systems into a single policy (Warnock, 2007)
Announcement	People directed	Use covert surveillance only in situations when there is proof that there has been wrongdoing (Goodwin, 2003).

CONCLUSION

OSN sites have many advantages; however, they also bring up serious legal and ethical issues. From the viewpoint of legal consequences, the businesses have to deal with a complicated set of rules relating to data protection, defamation, and intellectual property rights. Furthermore, common sense of ethics requires protecting user privacy, dispelling false information, and refraining from discriminatory actions. A misconduct of ethical norms can cause consumer reaction in the form of boycotts, decline public confidence, and may damage the brand's name. In order to decrease these risks, companies need to implement strong legal and ethical policies. Creating clear strategies, putting data protection in place, carrying out frequent audits, and educating staff members about ethical standards are all part of this. The key recommendations in this regard are as follows:

1. Creating an OSN strategy based on the type of business, and establishing objectives and Key Performance Indicators (KPIs).

2. Selecting the appropriate social media channels and conducting research on the intended audience.
3. Providing timely, interesting, and educational content that benefits both staff members and clients.
4. Responding to any comments, queries, and feedback on social media to provide excellent customer service.
5. Creating monitoring streams to find comments about a business on different channels.
6. Utilizing one's company's OSN sites to expand their business; it may help them to create, lead, enhance audience engagement, and raise brand awareness.

In addition, encouraging appropriate OSN site use in Pakistan requires cooperation with civil society organizations, industrial groups, and government authorities. In conclusion, the corporate OSN sites in Pakistan are subject to a continuously changing legal and ethical environment. Corporations may exploit the power of these platforms while protecting their interests and making a responsible contribution to a responsible digital ecosystem by acknowledging and resolving these challenges.

In Pakistan, the topic of the moral and legal consequences of corporate OSN sites is vibrant and always changing and demands further research. As new technologies such as artificial intelligence (AI), blockchain, and the metaverse continue to shape the digital landscape, it is crucial to examine their implications for legal and ethical considerations for corporate OSN sites in Pakistan. The development of a comprehensive and effective regulatory framework for corporate OSN in Pakistan is a matter of great priority and demands urgent attention. Researchers can contribute to the design and implementation of such a framework, taking into account international best practices and the unique context of Pakistan. Protecting the consumers from online troubles (such as misinformation, disinformation, and cyberbullying) is a critical concern, and it is very important to explore effective strategies for enhancing the consumer protection in the context of corporate OSN sites. Addressing the complex issues surrounding legal and ethical consequences of corporate OSN sites requires a multidisciplinary approach. Future research can benefit from collaborations between legal scholars, computer scientists, sociologists, and other experts. By focusing on these areas, researchers can contribute to a deeper understanding of the legal and ethical challenges faced by corporations operating in the digital age.

REFERENCES

American Civil Liberties Union (2008, February 8). Online Privacy Statement. Accessed August 7, 2009 at http://www.aclu.org/infor/18864res20050401.html.

Americans with Disabilities Act, 42 U.S.C. §§ 12101 et seq (1990). AmJur 2d (2009). Employment Relationship, 27, § 381.

Attaway, M. C. (2001). Privacy in the workplace on the web. Internal Auditor, 58, 30-35.

Baskin, M. (Winter, 1998). Is it time to revise your employee handbook? Legal Report, Alexandria Virginia: Society for Human Resource Management.

Benedict, J. (2008-2009). Deafening Silence: The Quest for a Remedy in Internet Defamation.

Cumberland Law Review, 39, 475.

Bersin, J. (2007, November 16). Social networking: meet corporate America. Accessed February 9, 2009 from http://joshbersin.com/2007/11/16/social-networking-meets-corporate-america/.

Blakely v. Continental Airlines, Inc., 751 A.2d 538 (N.J. 2000).

Boehle, S. (August, 2000). They 're watching you: workplace privacy is going, going…. Training, 37, 50-60.

Bonfield, B. (2008, January 8). Should your organization use social networking sites? Accessed February 9, 2009 from http://www.techsoup.org/learningcenter/internet/pages7035.cfm.

Brandenburg, C. (2008, June). The Newest Way to Screen Job Applicants: A Social Networker 's Nightmare. Federal Communications Law Journal, 60, 597.

Bureau of National Affairs (2009).

BNA Employment Guide. Washington, D. C.: Bureau of National Affairs.

Byrnside, I. (2008, Winter). Six Clicks of Separation: The Legal Ramifications of Employers' Using Social Networking Sites to Research Applicants.

Vanderbilt Journal of Entertainment and Technology Law, 10, 445.

Camardella, M. (2003). Electronic monitoring in the workplace. Employee Relations Today, 30,91-100.

Candilis, P. J. (2002). Distinguishing law and ethics: a challenge for the modern practitioner.

Psychiatric Times, 19 (12). Accessed September 8, 2005 at http://www.psychiatrictimes.com/ethics.html.

CIO Insight (2009). Five reasons to deploy a corporate social network Accessed February 9, 2009 at

http://www.cioinsight.com/c/a/past-news/5-Reasons-to-Deploy-a-Corporate-Social-Network/.

Clineburg, Jr., W.A. and Hall, P.N. (2005). Addressing Blogging by Employees. The National Law Journal.

Communications Decency Act, 47 U.S.C. §§ 652 et seq (2000).

Communitelligence.com (2009). Building Employee Branding and Engagement with Internal Social Networks. Accessed March 3, 2009 from http://wwwl.communitelligence.com/content/ahpg.cfm?spgid=361&full=1.

Coyote Communications (2008, November 27). Nonprofit Organizations and Online Social Networking: Advice and Commentary. Accessed August 7, 2009 from http://www.coyotecommunications.com/outreach/osn.html.

Deschenaux, J. (2009, March 12). Dealing With Employees 'Offensive Blogs and Facebook Postings. Accessed March 16, 2009 from http://www.shrm.org/legalissues/stateandlocalresources/pages/offensiveblogsfacebook.htm.

Dessler, G. (2009). Fundamentals of Human Resource Management. Upper Saddle River, N. J.: Pearson.

Ethics Scoreboard (2009, March 4). Untitled. AccessedMarch 20, 2009 from http://www.ethicsscoreboard.com/list/facebook.html.

Fair Labor Standards Act, 29 U.S.C. §§ 215 et seq (1949). Family and Medical Leave Act, 29 U.S.C. § 2601 et seq (1993).

Gabel, J.T.A. and Mansfield, N.R. (2003). The Information Revolution and Its Impact on the Employment Relationship: An Analysis of the Cyberspace Workplace. American Business Law Journal, 40, 301.

Gely, R., Bierman, L. (2006, Summer). Workplace Blogs and Workers 'Privacy. Louisiana Law Review, 66, 1079.

Glazowski, P. (2008, August 30). Biz networking on Facebook could soon supersede LinkedIn. Accessed February 9, 2009 from http://mashable.com/2008/08/30/b2b-ad-networking/.

Goodwin, B. (2003, June 17). Tell staff about e-mail snooping or face court, new code warns.
Computer Weekly, 38, p.5.

Graham, J. (2009, March 31). Marketers Find Twitter a Tweet Recipe for Success. Accessed April 1, 2009 from http://www.usatoday.com/tech/news/2009-03-31-facebook-twitter-status-marketing_N.htm.

Greenbaum, K. (2008, October 6). Ethics of Facebook Friendship: Can It Really Be a Conflict? Accessed March 20, 2009 from http://www.igreenbaum.com/20089/10/ethics-of-facebook-friendship-can-it-really-be-a-conflict/. Greenbaum, W., Zoller, B. (2006, July/August). Court Decisions Impact Workplace Internet and E-Mail Policies. HR Advisor.

Grubman, S. R. (2008, Winter). Think Twice Before You Type: Blogging Your Way to Unemployment. Georgia Law Review, 42, 615.

Gutman, P.S. (2003, Fall). Say What? Blogging and Employment Law in Conflict.
Columbia Journal of Law and the Arts, 27, 145.

Hawk, S. R. (1994). The effects of computerized performance monitoring: an ethical perspective.
Journal of Business Ethics, 13, 949-958.

Higgins, M.A. (2002, Spring). Blakey v. Continental Airlines, Inc.: Sexual Harassment in the New Millennium.
Women's Rights Law Reporter, 23, 155.

Hong, John S. (2007, Winter). Can Blogging and Employment Co-Exist?
University of San Francisco Law Review, 41, 445.

James, G. (2004, March). Can 't hides your prying eyes. Computerworld, 38, 35-36.

Kaupins, G. E. (2004), Ethical perceptions of corporate policies associated with employee computer humor.
Ethics and Critical Thinking Quarterly Review, 2004(1), 16-35.

Kaupins, G. E. & Minch, R. (2006, July-September). Legal and ethical implications of employee location monitoring.
International Journal of Technology and Human Interaction, (with Robert Minch), 2, 16-35.

King, N. J. (2003, Summer). Labor Law for Managers of Non-Union Employees in Traditional and Cyber Workplaces.
American Business Law Journal, 40, 827.

Kirkland, A. (2006, Winter). ―You Got Fired? On Your Day Off?!: Challenging Termination of Employees for Personal Blogging Practices. University of Missouri-Kansas City Law Review, 75, 545.

Kirkpatrick, D. L. & Kirkpatrick J. D. (2006). Evaluating Training Programs: The Four Levels (3rd ed.), San Francisco: Berrett-Koehler.

Kirkpatrick, M. (2008, July 17). Corporate Social Networks are a Waste of Money, Study. Assessed February 9, 2009 from http://www.readwriteweb.com/archives/corporate_social_networks_are.php.

Konop v. Hawaiian Airlines, Inc., 302 F.3d 868 (9th Cir. 2001).

LegalAndrew.com (2007). Facebook Isn't Private, and 7 Other Things You Should Know.
Accessed July 24, 2009 from
http://www.legalandrew.com/2007/07/21/facebook-and-the-law-8-things-to-know/.

Lex, R., (2007-2008). Can Turn into My Lawsuit? The Application of Defamation Law to Online Social Networks. Loyola of Los Angeles Entertainment Law Review, 28, 47.

Lichtenstein, S.D., & Darrow, J.J. (2006, Fall). Employment Termination for Employee Blogging: Number One Tech Trend for 2005 and beyond, or a Recipe for Getting Dooced?
UCLA Journal of Law & Technology, 2006, 4.

McCain, R. S. (2009). Facebook Ethics. The other McCain. Accessed March 20,2009 from http://rsmccain.blogspot.com/2008/03/facebook-ethics.html.

McCarthy, C. (2009, April 8). Facebook Hits 200M Users, Looks to Charity. Accessed April 9, 2009 from http://www.cbsnews.com/stories/2009/04/08/tech/cnettechnews/main4930230.shtml.

Milligan, Tanya E. (2009, February). Virtual Performance: Employment Issues in the Electronic Age. Colorado Lawyer, 38, 29.

National Labor Relations Act, 29 U.S.C. §§ 151-169 (1947).

National Work rights Institute (2004). Electronic Monitoring in the Workplace: Common Law and Federal Statutory Protection. Accessed October 12, 2004 at: http://www.workrights.org/issue_electronic/em_common_law.html.

Nolan, D. R. (2004). Privacy and profitability in the technological workplace. Journal of Labor Research, 24, 207-232. Occupational Safety and Health Act, 29 U.S.C. §§ 651 et seq (1970).

Organization for Economic Cooperation and Development, (2000). OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, Paris: OECD Publication Service, Accessed October 12, 2004 at: http://www1.oecd.org/publications/e-book/9302011E.pdf.

Ostrow, A. (2009, March 9). Social networking more popular than email. Accessed April 10, 2009 from http://mashable.com/2009/03/09/social-networking-more-popular-than-email/.

Owyang, J. (2009). What Facebook Connect means for corporate websites. Accessed February 9, 2009 from: http://www.web-strategist.com/blog/2008/07/23/what-facebook-connect-means-for- corporate-websites/.

People Management (2007, November 15). Facebook-style site attracts staff on rebound. People Management, 13, 12.

Porter, W. G. and Griffaton, M. C. (2003). Between the devil and the deep blue sea: monitoring the electronic workplace. Defense Counsel Journal, 65-77.

Raphael, J. R. (2009). People Search Engines: They Know Your Dark Secrets…and Tell Anyone. Accessed March 30, 2009 from: http://tech.msn.com/products/articlepcw.aspx?cp-documentid=18632762&GT1=40000.

Sarbanes-Oxley Act, 18 U.S.C. §§ 2510-2522; 2701-2711 (2002).

Schultz, J. (2008, November 25). Facebook Creeping! The Ethics Involved with Employers Usage of Facebook. Accessed August 7, 2009 at http://www.jaytaylorschultz.com/PDFs/Research-Facebook-Creeping.pdf.

Securities and Exchange Act, 15 U.S.C. §§ 78 et seq (1934).

Sims, R. R. (2003). Ethics and Corporate Social Responsibility: Why Giants Fall, Praeger, Westport, Conn.

Sprague, R. (2008, Fall). Orwell Was an Optimist: The Evolution of Privacy in the United States and its De-Evolution for American Employees. John Marshall Law Review, 42, 83.

Sprague, R. (2007, Winter). Fired for Blogging: Is There Legal Protections for Employees Who Blog? University of Pennsylvania Journal of Labor and Employment Law, 9, 355.

Strege-Flora, C. (2005, Autumn). Wait! Don ‘t Fire That Blogger! What Limits Does Labor Law Impose on Employer Regulation of Employee Blogs?

Shidler Journal of Law, Commerce & Technology, 2, 11.

Sutter, J. D. (2009). Are Twitter ‘s Breakneck Growth Causing a Backlash? Accessed March 31,2009from: http://www.cnn.com/2009/TECH/03/31/twitter.fail.whale/index.html?iref=t2test_techtues.htm

Title VII of the 1964 Civil Rights Act, 42 U.S.C. §§ 2000d et seq (1964).

Urban Dictionary (2008, September 18). Facebook Ethics. Accessed August7, 2009, at http://www.urbandictionary.com/define.php?term-facebook%20Ethics.

Warnock, O. (2007, September 26). Networking or not working? Contract Journal, 440, 31-32.