Business Management Dynamics
Vol.3, No.10, Apr 2014, pp.28-36

Privacy: Expectations and Employment

Janice M. Karlen, Ed.D.[1]

Abstract

The increased collection and perusal of personal information gleaned from social media platforms by government, data brokers, businesses, and the global community has spurred concern regarding the issue of individual privacy. This study examines general user privacy, privacy rights, and concerns of employees both in and outside of the workplace and those of prospective employees in the recruitment process. Industry self-regulation and government oversight are discussed as are options for organizations and individuals to be proactively responsible for their privacy.

Key words: Privacy, Social Media, Employment

Available online
www.bmdynamics.com
ISSN: 2047-7031

INTRODUCTION

As technology and social media platforms have developed and become part of common experience, individuals have had to consider the meaning of privacy in a continuously changing environment that is vastly different than in the past. Information that used to be closely held by friends and family is now available to millions without any consideration of the implications. Organizational leaders must give attention to the privacy expectations of individuals in society in general and in their relationships with business as applicants, employees, and customers.

The growth in social media reflects general trends towards the emergence of a more connected world where people can share and find information quicker and more conveniently. However, this means that "privacy has become over the last decade one of the foremost social concerns, since the arrival of cheap and ubiquitous surveillance of both online and offline behavior" (Orzan et al, 2012). Social media technologies in particular facilitate access to intimate knowledge about individuals that is increasingly used by managers and agencies for marketing, surveillance and recruitment purposes. However, the emergence of these types of social media usage is somewhat controversial, as many individuals and lawmakers argue that there are privacy issues surrounding the use of the information gathering techniques utilized. In the United States, recent issues have emerged challenging the tendency of potential employers to demand access to individuals' social media passwords as part of the recruitment process, with questions regarding the extent to which this practice violates federal law, including the Stored Communications Act and the Computer Fraud and Abuse Act (del Riego et al, 2012). Consideration of how expectations of privacy have changed as a result of the increased use of social media, and the implications for both corporate managers and users of social media are discussed. Three main areas: general user privacy, employee privacy, and the privacy of potential employees during the recruitment process are addressed.

GENERAL USER PRIVACY

According to "Worldwide Social Network Users: 2013 Forecast and Comparative Estimates," nearly one in four people worldwide will use social networks in 2013 ("Social Networking Reaches", 2013). The Pew Research Center's Internet & American Life Project reports that as of May 2013, 72% of online adults in the United States use social networking sites, and 18% use Twitter (Brenner & Smith, 2013). In addition to personal usage, more businesses are taking advantage of the benefits that social media sites offer. In a study by global management consulting firms Booz & Company and Buddy Media, it was found that 96 percent of companies surveyed plan on increasing their investments in social media. Advertising and promotions, public relations, and customer services were listed as the main uses or benefits though other uses such as market research and recruitment were reported.

[1] *City University of New York, Director of Business Programs and Professor*
E-mail: jkarlen@lagcc.cuny.edu

Social media has aided individuals to follow their family, friends, celebrities and random others. Businesses can delve further into the privacy areas of potential and current employees and consumers than ever before. This is primarily because people use social media to announce what they are doing, who they are communicating with, where they are and a myriad of other details of their personal lives. They blog about their opinions and publicize their plans. At the same time, many individuals are concerned with issues of identity theft and inappropriate use of their personal information.

Microsoft Trustworthy Computing division released data in 2012 from a survey of 5,000 people whose online behaviors and attitudes vary widely and how their actions impact their overall online profiles and reputations. Fourteen percent of people believe they have been negatively impacted by the online activities of others, even unintentionally so. Of those, 21% believed it led to being terminated from a job, 16% being refused health care, 16% being turned down for a job, and 15% being turned down for a mortgage (Lynch, 2012).

In general, social media is very conducive to businesses looking to improve interaction with their customers. One of the most wide spread of these focuses on social media to track people who 'like' a certain product, and tweets or blog about a company or one of their products would be included (Kumar and Sundaram, 2012). On the one hand, these processes and activities are seen as part of the interaction between companies and their consumers in the digital age. However, at the same time there are also concerns around the extent to which companies such as Facebook and Google are using this data in marketing activities without the consent, or even the knowledge, of consumers. One example is a recent consumer backlash against Google, after the company launched a service which would have included the faces, comments and profiles of individuals in paid-for corporate advertisements (BBC, 2013). This created controversy due to the potential for people's images and posts on Google's review sites to be used without their consent, in an effort to gain profit for the company. A similar issue emerged when Facebook began using people's profiles in 'sponsored stories', which was ruled to have violated their privacy as it was done without permission (BBC, 2013).

These examples clearly demonstrate that users of social media sites expect their details to be kept private and used exclusively by them, and that the law will often lend support if these expectations are violated. However, while the case of Facebook shows that users do have some power in this area, Google's approach is arguably more insidious to privacy, as the company is informing customers of a change in its use of their data in advance, and requiring them to opt out if they object (BBC, 2013). This demonstrates that Google recognizes the privacy rights of its users and that the law requires that that consent must be obtained. Google is looking to secure this consent in an implied manner. Such an issue raises the importance of "the need to check the privacy settings on social networking sites" and ensures that implied permission is not given if the user does not wish it to be (Mitchell, 2013). This is an issue which arguably transcends business, with many U.S. based technology firms and social media sites sharing their customer data with security agencies even if the user objects and raises a separate legal issue around the extent to which the Fourth Amendment protections against search and seizure are applied to meet reasonable expectations of privacy with social media (Sanvenero, 2013). This issue has not yet been resolved by the U.S. courts, thus while users may expect that their private information will always remain private; this is not always the case.

Additionally, even when a social media company keeps its users' data private and does not use it in a public manner, some privacy issues may still surface. In particular, Fong (2010) reports "that social media, such as Facebook, has allowed businesses in British Columbia to develop products and services needed by consumers" using those consumers' data." In particular, companies such as Facebook will use data to provide companies with information to assist them in personalizing advertisements and services that they offer to these consumers. While the third parties will not necessarily learn identifiable data about users, they may still obtain enough information to develop personalization strategies which can be used to target individuals with advertisements and content (McEleny, 2011). This strategy forms part of a trend known as 'hyper-personalization' in marketing, through which consumer behavior data and filtered information from electronic commerce sites are used to target individual customers (Woods, 2012).

It can be argued that this is not in line with consumer expectations of privacy, as discussed by the BBC (2013) and others. However, many consumers continue to inadvertently support these forms of campaigns through their use of programs such as Facebook Beacon, which asked online buyers if they want to include details of purchases and business transactions to their Facebook profile (Tsai, 2008). Facebook Beacon was subsequently shut down in 2009, with the CEO Mark Zuckerberg admitting in 2011 that it had been a mistake. While individuals may use these types of services to inform their friends of their purchases and activities, it is also used by businesses. Marketing databases are created that allow building of an improved picture of the purchasing activities of individuals in order to better market to them. Again, users have the choice to opt out of these services, but the fact that many do not indicates that individuals are not fully aware that their privacy expectations are not being met by many companies. Failure to opt out leaves individuals vulnerable to having data they expect to be private used by companies for marketing and advertising purposes. While this does not seem to be a grave violation of privacy, developments in social media technology have led to the use of new technologies including facial and body recognition systems (Mennecke and Peters, 2013). These are likely to have more significant privacy implications as companies and third parties are able to obtain biometric and other data from users who fail to opt out. At Reebok's flagship store in New York City, for example, there is already a face-detection system in place that is able to determine a shopper's gender, age, and interest in particular items. The system called Cara was installed in May 2013. At this time, the system does not match a face with ones in a database; it only extracts demographic and behavioral data and then destroys the image fractions of seconds later (Sofge, 2014). Shoppers do not know that they are participating and may not opt out. The natural progression of this kind of observation is the potential for matching images with those available in the public media sphere.

As these technologies become more widespread, it is reasonable to expect that customer expectations and demands around privacy in social media would increase accordingly. However, this may not be the case for all consumers. In 2014, IBM announced the result of a study that indicated that consumers indicated their willingness to share personal information with retailers that they trusted and who would give them "good value" for sharing that information. "The percentage of consumers willing to share their current location via GPS with retailers nearly doubled year-over-year to 36 percent. Thirty-eight percent of consumers would provide their mobile number for the purpose of receiving text messages and 32 percent would share their social handles with retailers." (IBM, 2014).

EMPLOYEE PRIVACY

During the employment relationship, the issue of privacy is one that consists of laws which are vague and not commonly known. The implication is that privacy issues are relegated to employer discretion that is guided by modest legal requirements. Selmi (2006), Lasprogata *et al* (2004) and Sprague (2008) delve into the areas of subjective and objective expectations of privacy from a legal perspective. In an article by Sprague (2008) he makes the statement that "Employees have virtually no privacy". In support of this, Sprague (2008) states that applicants are screened through resume and employment checks, where databases are used to confirm prior employment and personal histories. He adds that emails may be monitored, and in today's social media age, employee postings on social media sites can serve as information content that employers can access and use in their employee investigations. In terms of employees in the workplace, most firms keep database records of computer keystroke activity, Internet addresses visited and phone numbers dialed. Other practices include video monitoring in the workspace, using GPS to track company vehicles, and reading emails originating from company computers whether they are from company or personal accounts.

Similarly, information stored or held on third party electronic devices that are publically accessible, such as social media, websites, etc. have privacy issues governed by the policies of the companies that own and manage these sites (Hodge, 2006). Some employers may use social media monitoring tools like Trackur or Social Intel to monitor employees as well as their own company's reputations.

While the social media activities of all individuals are potentially used by companies and managers for external marketing and business reasons, there is also a growing trend for social media usage to affect the employee and employer relationship. This is increasingly the case as the use of social media in the United

States and other developed nations' workplaces is on the rise, with people using social networks to discuss employment related issues, and companies monitoring the use of the internet by their employees (Mello, 2012). In general, the vast majority of modern businesses have policies regarding how employees can use social media in the context of their work, and what an employee can say about the company online. However, at the same time, Sánchez Abril et al (2012) argue that "despite granting employers access to information about their private lives by participating online, respondents expect that work life and private life should be generally segregated—and that actions in one domain should not affect the other". This raises an obvious conflict over the extent to which the ability of employers to access and control employees' activities on social media is in line with employee expectations of their right to privacy.

In general, according to Barron (2012), many issues in this area can be addressed by ensuring that employees are informed about the company's policies on using social media, and that these policies are reasonable. For example "it is unlawful if a manager inquires about personal information displayed on social sites in the workplace" however "an employer has the right to search the cell phone of an employee if there is notice in its policies that employees have no expectation of privacy for information" (Barron, 2012). Other issues are more clear cut, such as the case of a tweet sent by an employee from the official @ChryslerMotors Twitter account which stated "I find it ironic that that Detroit is known as the #motorcity and yet no one here knows how to f---ing drive", which resulted in the employee being fired (Gross, 2012). In such a case, an employee using an official account and clearly affiliating themselves with the company could obviously have no expectations of privacy.

However, at the same time there are potential conflicts of interest between employers and employees regarding the use of social media in a non-official capacity. According to Hunt and Kessler (2013), lifestyle discrimination statutes protect an employee's right to use Facebook and other social media sites to pursue their private lives in any way they wish, so long as this does not interfere with their ability to do their job. However, when their personal activity relates to their work then the borders can become more blurred. In some cases, such as the BBC, social media policies quite clearly distinguish between personal activity which is not done in the name of the BBC, official BBC activity, and personal activity which relates to the BBC. It is the last of these categories that is the most divisive, due to the potential reflections on the organization.

In another example, the United States Air Force encourages its employees to 'stay in their lane' or area of expertise, with a policy stating "If you're an aircraft mechanic, you're well suited to communicate messages about aircraft maintenance… If you're an aircraft mechanic blogging about legal issues -- reconsider your blog" (Gross, 2012). There is obviously an argument here that an employee has the right to blog in a personal capacity regardless of their expertise, and the right to do so is legally protected unless it has an obvious negative impact on their employer. However, as IBM notes, its employees should "be aware of your association with IBM in online social networks. If you identify yourself as an IBMer, ensure your profile and related content is consistent with how you wish to present yourself with colleagues and clients" (IBM, 2013). This shows perhaps the most challenging aspect of personal social media usage: if an individual uses a public social media site to present themselves as having certain views or opinions then their employer, colleagues and clients can easily access these opinions, and may form judgments which influence the individual's career.

Another important issue in this area is the extent to which employees are protected from retribution when they share thoughts and opinions about job conditions with coworkers. While many companies try to prevent their employees from doing this, Gross (2012) notes that employees do have the right to complain about their job if their complaint is intended to address a specific issue. However, "whining about them to anyone who will listen can still get you fired, especially when it happens on a platform that can spread those complaints all over the world in seconds" (Gross, 2012). Company policies are generally falling in line with these requirements, with Wal-Mart's policy only acting to prevent "inappropriate postings that may include discriminatory remarks, harassment and threats of violence or similar inappropriate or unlawful conduct" (Greenhouse, 2013). However, in the case of General Motors, the company's social media policy contains instructions that "offensive, demeaning, abusive or inappropriate remarks are as out of place online as they are offline" (Greenhouse, 2013). This may be seen as an example of a bad policy as it attempts to prevent employees from voicing protected criticisms of labor policies or the treatment of employees. However, it is important to note that if these comments are made on a public site then the employee cannot expect privacy-- while risking possible retaliation from colleagues and management viewing these comments--even though legal action is not permissible.

RECRUITMENT PRIVACY

Expectations of privacy when using social media do not necessarily fall in line with practice and law in the realm of social media use during recruitment. According to Watt (2013), companies increasingly use social media to attract employees, but also to screen them. Specifically, recruiters will seek to access social media profiles to understand the attitude, appearance, behavior and professionalism of potential recruits, and screen out individuals who do not appear to fit with the company’s desired profile of employees. Ideally human resource professionals want this method to be a force for “good” in not only the more obvious areas of recruitment and selection but also areas such as motivation and team-building (Alastair, 2013). Again, this will create conflicts due to expectations of individuals who create social media profiles and share intimate aspects of their private lives without giving sufficient thought to how potential employers may view their information. This is an area in which “candidates need to be increasingly aware that unless they have their privacy setting correctly adjusted, potential employers can see a good deal of what they are up to” (Watt, 2013). This is a significant grey area, with employment bodies arguing that employers could potentially face lawsuits for discrimination if they reject individuals purely based on their social media profile. However, in modern recruiting with huge numbers of candidates and criteria, it is often very difficult to determine or prove the precise reason why a specific candidate was rejected, unless they were applying for a very specific job out of a narrow pool of applicants.

A more worrying trend, from a privacy point of view, is that companies are increasingly requesting access to the Facebook and other social media accounts of applicants, despite this being a violation of Facebook’s own policies (Horn, 2012). In theory, individuals have the right to refuse to hand over their password. However, in practice many individuals expect that this will result in them no longer being considered for the position, and thus they tend to comply (Del Riego et al, 2012). Individuals who refuse and then are not selected also face similar issues to those discussed in the previous paragraph, namely being unable to prove that their rejection was due to their refusal to hand over their log in details. This represents an area in which expectations are clearly not in line with practice, as individuals who are technologically aware may set their privacy settings to prevent potential employers from accessing their social media profile, only to find they have to grant access anyway. Fortunately, from a privacy point of view, laws in this area are beginning to be tightened. For example, “in September 2012, California Governor Edmund G. Brown Jr. signed two bills into law prohibiting employers and universities from demanding the e-mail or social media account passwords of applicants” (Thompson, 2012). More recently “the states of Utah, New Mexico, and Arkansas have passed laws that prohibit employers from requiring or even requesting access to job applicants' social media profiles in 2013” (Deschenaux, 2013). Thus, this is an area in which the legal situation is rapidly catching up with privacy expectations.

Despite the progress made in this area, there are still over forty US states in which potential employers have the ability to demand access to social media sites, even those protected by passwords or privacy settings, as part of the recruitment process (Deschenaux, 2013). However, as individuals become more aware of these types of screening techniques, they have become better able to counter these measures. For example, many individuals have increasingly begun creating multiple social media profiles on sites such as Facebook. Some of these profiles are kept private and completely hidden from the view of all but the individual’s friends, while others are ‘sanitized’, or even enhanced through the addition of information designed to increase the apparent attractiveness of the candidate (Davison et al, 2011). This has resulted in managers being more aware of the advantages and disadvantages of using social media information for applicant screening (Slovensky and Ross, 2012). As such, this is an area in which the users of social media sites are potentially able to protect their privacy, provided they are cognizant of management’s practices.

Examples of practices for good leadership

In the United States, restrictions related to privacy concerns have been allowed to remain vague, while laws and policies in the European Union (EU) were developed to enhance consumer and employment privacy protections.In the EU, background checks are restricted concerning what can and cannot be used and obtained (Wugmeister and Bevitt, 2008). The monitoring of employee activity in the workplace is considerably more lax in Europe, which relies on the moral adherence of employees to observe the workplace employee/employer relationship under an aura of mutual trust (Mitrou and Karyda, 2006). The European Commission announced in January 2010 that it was planning the development of a series of comprehensive new laws regarding social media and Internet privacy (Phillips, 2010). This was in direct response to a statement made by Mark Zuckerberg of Facebook who stated "… no one cares about privacy anymore …" (Phillips, 2010). While that statement sparked a wave of protest in cyberspace, its impact in the United States with respect to government action has been basically non-existent. There has been slow but steady progress in the EU to approve regulations that would afford individuals, in their personal and employment roles, more social media privacy protection. Included in the proposal are rules that would affect storage and use of data collected via social media by third party countries e.g. the United States.

The National Labor Relations Board (NLRB) developed a number of rulings concerning employer policies in relation to social media. The NLRB recently made the announcement that the varied instances are fact specific and offered the following guidance regarding monitoring and use of viewed information, stating: The policies of employers "… should not be so sweeping that they prohibit the kinds of activity protected by federal labor law, such as the discussion of wages or working conditions among employees" (Dolan *et al*, 2013). This guidance and other examples available from the NLRB can form the beginning for the development of a good social media policy for business organizations.

Knowing what activities are protected, and which ones are not, is valuable information as organizations develop policies that are not overbroad, ambiguous, and enforceable. Cautioning employees that all corporate-owned equipment and technology will be monitored is a beneficial first step, to be followed by forewarning and training about such behavior as posting comments that disparage other employees or leaking confidential organizational information. Business leaders need to understand that claims of defamation, discrimination or creation of a hostile work environment may emanate from poorly understood requirements and inadequately trained staff.

According to the Privacy Rights Clearinghouse (2013b), there are ten states where legislation protects job applicants and employees from requests from employers that the user names or passwords from individual social media accounts be turned over to management. It is an obligation of management to know these protections to keep the organization from inadvertently becoming a violator, and subject to penalty.

IMPLICATIONS, RECOMMENDATIONS AND SUGGESTIONS

It is demonstrated how the increased use of social media has had significant impacts on the privacy of individuals. However, expectations of privacy have been relatively slow to catch up with these impacts. In particular, many individuals continue to expect that the information they place on social media websites will be private, and not exploited by companies or employers, either actually or potentially. The evidence from this study has indicated that this is not the case, and despite the existence of laws designed to prevent abuse, this information is widely accessed and used by companies for a range of purposes. The solution to this issue from the perspective of individuals is to become more aware of the potential publicness of their personal information and to moderate their expectations of privacy in universal media. People need to take responsibility for knowing how to keep their private information truly private and not rely upon external organizations to protect them. In particular, individuals need to ensure that they regularly check their settings to ensure their chosen level of privacy matches their expectations, and they are not implying any consent by their actions, as well as regularly managing their accounts to prevent potential employers from viewing private information. Privacy expectations, and the actions taken to guarantee privacy in social media usage, will change as individuals become more informed and knowledgeable regarding the privacy impacts of social media use.

Although the Federal Trade Commission (FTC) called for reform regarding social media privacy, the issue has been essentially left to industry self-regulation. One result of this was the development of the Self-Regulatory Principles for Online Behavioral Advertising (2009) by the Interactive Advertising Bureau (IAB). In addition to proposing seven principles for member conduct regarding collection and promulgation of consumer information, the IAB has developed a beta site where consumers can opt out from customized advertising by member organizations. More recently, the FTC has recommended the use of a "Do Not Track," option much the same as the "Do Not Call" option for telephone customers, however there has been no action to date.

From the corporate perspective, companies failing to provide employees with a widely communicated and lawful allowable-use social media policy are risking legal and ethical complications, according to Millennials, Social Media, and Employee Usage, a white paper from Corpedia Inc., a Phoenix-based governance, risk, and control education and consulting firm (Steffee, 2012). Furthermore, inappropriate use of social media in the employment process and without sufficient procedure and controls may leave an organization open to complaints of discrimination. While difficult to prove, such allegations are damaging to the organization and may be expensive to defend. Also, depending on the ways that information acquired via social media is maintained, an organization may be subject to requirements of the Fair Credit Reporting Act. The ramifications of that include maintaining records retrieved from public sites for a period of up to seven years along with the obligation to revise or change information if corrections are made to the original records.

In 1985, Spiros Simitis, Germany's leading privacy scholar and practitioner gave a lecture at the University of Pennsylvania Law School. He recognized that privacy is not an end in itself, but a means of achieving a certain ideal of democratic politics, where citizens are trusted to be more than just self-contented suppliers of information to all-seeing and all-optimizing technocrats. "Where privacy is dismantled," warned Simitis, "both the chance for personal assessment of the political … process and the opportunity to develop and maintain a particular style of life fade."

Three technological trends underpinned Simitis's analysis (1985). First, he noted, even back then, every sphere of social interaction was mediated by information technology—he warned of "the intensive retrieval of personal data of virtually every employee, taxpayer, patient, bank customer, welfare recipient, or car driver." As a result, lack of privacy was no longer solely a problem of some unlucky person caught off-guard in an awkward situation; it had become everyone's problem. Second, new technologies not only were making it possible to "record and reconstruct individual activities in minute detail" but were also normalizing surveillance by weaving it into the fabric of our everyday life. Third, the personal information recorded by these new technologies was allowing social institutions to enforce standards of behavior, triggering "long-term strategies of manipulation intended to mold and adjust individual conduct." That this observation was made over twenty-five years ago with the technology of that time was particularly prescient.

While Americans enjoy broad based freedom of speech and movement along with other rights, their concerns over privacy have received less attention. People may be worried about identity theft, but are less cognizant of the public availability of their location and their actions at the moment, and for the long term. While there are regulations that affect the activities of business organizations in the monitoring of individuals, in general, they are minimally understood and not acknowledged until there is a problem involving litigation or notice in the major media. As the European Union develops standards for individual privacy that may affect American organizations that collect, disseminate or use information obtained from social media sources, management should be proactively assessing their current activities and policies.

What remains a question regarding the word "privacy" is the issue of responsibility. In 2013, there was national outcry when Edward Snowden announced to the world that the United States government has been tracking and maintaining the telephone records and emails of millions of Americans. It was argued in the media that this was an invasion of privacy and that the National Security Administration did not have the proper authority to follow the communications of citizens nor to maintain records of these communications for the long term. It is interesting to note that information possessed by corporate marketers and employers about people's habits, preferences and personal behavior may be far more

reaching and revealing, and the very people who object to the government tracking them willingly “opt in” to corporate information gathering when they receive a 10 percent discount on their next purchase.
So what becomes the question for further study is, “Where is locus of control for privacy?” Is it the responsibility of the individual who may not realize the potential impact of social media both immediately and into the future? If laws are made that restrict information gathering and use, can it be expected that the government, which is itself in the information gathering business, will be the enforcer of these laws? Or, should we continue to pursue the industry-promoted policy of self-regulation?

REFERENCES

Alastair. (2013, October 11). How is Social Media Impacting Your Role in Human Resources? [Web log comment]. Retrieved from http://employee-relations.hr.toolbox.com/groups/strategy-administration/employee-relations/how-is-social-media-impacting-your-role-in-human-resources-5282898?reftrk=no&trdref=4e6577736c6574746572.

Brenner, J, & Smith, A. 72% of “Online Adults are Social Networking Site Users” August 5, 2013 Retreived from http://pewinternet.org/Reports/2013/social-networking-sites.aspx.

Barron, D. (2012) *Social Media: Frontier for Employee Disputes.* Baseline. 114, 14.

BBC (2013) http://www.bbc.co.uk/news/technology-24519300 Accessed 14th October 2013.

Davison, H. Maraist, C. and Bling, M. (2011) *Friend or Foe? The Promise and Pitfalls of Using Social Networking Sites for HR Decisions.* Journal of Business & Psychology. 26(2) 153-159.

Del Riego, A. Abril, P. and Levin, A. (2012) *Your Password Or Your Paycheck?: A Job Applicant's Murky Right To Social Media Privacy.* Journal of Internet Law. 16(3) 1-26.

Deschenaux, J. (2013) *Seven States Protect Social Media Privacy.* HR Magazine. 58(6) 16.

eMarketer June 18, 2013 Social Networking Reaches Nearly One in Four Around the World Retreived from http://www.emarketer.com/Article/Social-Networking-Reaches-Nearly-One-Four-Around-World/1009976#2SSIdHZRSxQXVme1.99.

Fong, P. (2010) *Privacy for Sale.* BC Business. 38(10) 40-45.

Greenhouse, S. (2013) http://www.nytimes.com/2013/01/22/technology/employers-social-media-policies-come-under-regulatory-scrutiny.html?pagewanted=all&_r=0 Accessed 14th October 2013.

Gross (2012) http://edition.cnn.com/2012/02/07/tech/social-media/companies-social-media/index.html Accessed 14th October 2013.

Hodge, M. (2006) Fourth Amendment and Privacy Issues on the New Internet: Facebook.com and Myspace.com. *Southern Illinois University Law Journal*. 31(8), 95-111.

Horn, L. (2012) *Facebook Condemns Those Requesting Passwords of Interviewees, Employees.* PC Magazine. 1.

Hunt, R. and Kessler, L. (2013) *Wanna Be Friends? The Potential Impact Of Lifestyle Discrimination Statutes On Employer Facebook Policies.* Journal of Legal Studies in Business. 18, 45-68.

IBM (2013) http://www.ibm.com/blogs/zz/en/guidelines.html Accessed 14th October 2013.

IBM (2014) http://www-03.ibm.com/press/us/en/pressrelease/42903.wss Accessed 23 January 2014.

Kumar, V. and Sundaram, B. (2012) *An Evolutionary Road Map to Winning with Social Media Marketing*. Marketing Research. 24(2) 4-7.

Lasprogata, G., King, N., Pillay. S. (2004) Regulation of Electronic Employee Monitoring: Identifying Fundamental Principles of Employee Privacy through a Comparative Study of Data Privacy Legislation in the European Union, United States and Canada. *Leland Stanford Junior University Stanford Technology Law Review*. 4(3), 23-35.

Lynch. (2012, January 24). Microsoft & Data Privacy Day: Put Your Best Digital Foot Forward [Web log post]. Retrieved from https://blogs.technet.com/b/microsoft_blog/archive/2012/01/24/microsoft-amp-data-privacy-day-put-your-best-digital-foot-forward.aspx?Redirected=true.

McEleny, C. (2011) *Sharing data among friends*. Marketing Week (01419285). 34(46) 32.

Mello, J. (2012) *Social Media, Employee Privacy And Concerted Activity: Brave New World Or Big Brother*? Labor Law Journal. 63(3) 165-173.

Mennecke, B. and Peters, A. (2013) *From avatars to mavatars: The role of marketing avatars and embodied representations in consumer profiling.* Business Horizons. 56(3) 387-397.

Mitchell, G. (2013) *Privacy is the currency of online retail, and it's too high a price to pay for what we're getting.* Engineering & Technology (17509637). 8(7) 26.

Mitrou, L., Karyda, M. (2006) Employees' privacy vs. employers' security: Can they be balanced? *Science Direct*. 23(3), 164-178.

Orzan, G., Veghes, C., Silvestru, C., Orzan, M., & Bere, R. (2012). Marketing Implications of Information Society Privacy Concerns. *Review Of International Comparative Management / Revista De Management Comparat International*, 13(5), 733-742.

Phillips, L. (2010) *New EU Privacy Laws Could Hit Facebook*. Retrieved from http://www.businessweek.com/globalbiz/content/jan2010/gb20100129_437053.

Sánchez Abril, P. Levin, A. and Del Riego, A. (2012) *Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee.* American Business Law Journal. 49(1) 63-124.

Sanvenero, R. (2013) *Social media and our misconceptions of the realities.* Information & Communications Technology Law. 22(2) 89-108.

Selmi, M. (2006) Privacy for the Working Class: Public Work and Private Lives. *Louisiana LawReview.* 66(5), 1-24.

Simitis, S. (1987) *Reviewing Privacy in an Information Society. University of Pennsylvania Law Review. 135(3)* 707-746.

Slovensky, R. and Ross, W. (2012) *Should human resource managers use social media to screen job applicants?* Managerial and legal issues in the USA. Info. 14(1) 55-69.

Sofge, E. (2014, January 15). The End of Anonymity. *Popular Science.* Retrieved January 19, 2014 , from http://www.popsci.com/node/134118/?cmpid=enews011614&spPodID=020&spMailingID=6017689&spUserID=OTc5Nzg4NDk4MQS2&spJobID=361691849&spReportId=MzYxNjkxODQ5S0

Sprague, R. (2008) Orwell Was An Optimist: The Evolution of Privacy in the United States and Its De-evolution for American Employees. *John Marshall Law Review.* 42 (2008): 83-134.

Steffee, S. Avoiding Social Media Catch 22s. *Internal Auditor,* 69 (5), 13-15.

Thompson, M. (2012) *Social Media, the Law, and You.* EContent. 35(10) 8-10.

Tsai, J. (2008) *Facebook's About-Face.* CRM Magazine. 12(1) 17-18.

Watt, G. (2013) *Recruitment profiling by social media.* Money Marketing. 3/21/2013, 54.

Woods, A. (2012) *Up close and very personal.* Marketing (00253650). 9/5/2012, 3-5.

Wugmeister, M., Bevitt, A. (2008) *Comparing the U.S. and EU Approach to Employee Privacy*. New York: Morrison & Foerster