



The Legal Aspect of Social Media Employment Background Check and its Implications for Employers

*Parichat Janthori**

Abstract

As the social networking sites such as Facebook, MySpace, and Twitter have become popular among students and new graduates, employers or recruiting organizations are using them as a tool in a recruiting process. The so called “background check” is increasingly conducted online through social networking sites, in many cases without permission. Online background check is viewed as a less expensive and effective tool to get the useful information about job applicants. However, this could contribute bias and discrimination in employment a decision making process since a number of employers reject job applicants because the information they have seen on the social networking sites. This article will discuss the legal aspect of social media employment background check, and aim to determine whether the background check in social networking sites violates the right to privacy of the job applicants and complies with law. Moreover, this article provides the implication for employers in order to avoid privacy right infringement.

Key words:

Social networking sites: A Web site that provides a virtual community for people such as Facebook, Hi5, or Twitter

Background check: The process of authenticating the information supplied to a potential employer by a job applicant in his or her resume, application, and interviews.

Personal data protection: The protection of individuals with regard to the processing of personal data and on the free movement of such data.

* Lecturer, Faculty of Commerce and Accountancy, Thammasat University.



Right to privacy: The right of a person to be free from intrusion into or publicity concerning matters of a personal nature

Introduction

Advanced information technology has changed the way how people communicate with each other. Internet enables people to contact or to talk to one another around the world with a very tiny cost, but in a lightning speed. Internet has a great impact on how business is conducted. It increases transparency in the marketplace and provides efficiency by reducing time for communication and enabling the business transactions to be undertaken at any time from everywhere. Hence, Internet is widely adopted in many parts of business organizations, for example, in human resource management functions. Human resource professionals use Internet in a recruiting process. It helps organizations to communicate with job candidates, to attract them, and it is increasingly used in employee scanning and selecting process. It was cited in several surveys that employers are increasingly performing online background check (Careerbuilder.com, Vault.com, Society of Human Resource survey). This refers to the act of reviewing both confidential and public information to investigate a person or entity's history. As an extensive background check is quite expensive mainly because of the time and effort necessarily used in exploring every item in a person or entity's history, employers are checking job candidates' background through information provided online, particularly in social networking sites (SNSs), as these SNSs provide a less expensive and quick source of background information. Since the information, pictures or any posts in the SNSs may have an impact on hiring decisions; it could cause bias against job candidates. People start questioning the privacy issue in social networking sites and legal right of the employers to perform online background check and whether this is ethical for employers to use social profile information as a factor in hiring decisions.

This article will provide an overview on how social networking sites are used in a recruiting process and explore some of the legal issues raised when online background check is conducted. It must be noted that this article will focus on the Facebook social network and its users.



The first section of this article will describe the social networking sites and how it is used as a tool for background check. The next section discusses the key legal issue relating online background check, namely the right to privacy. The conclusion and guidelines for employers how to conduct legally background check in the Internet will be provided in the last section of this article.

1. Social networking sites and online background check

Social networking sites or Web 2.0 represent a new stage of an online communication tool. It has become increasingly popular among the general population, especially among college students and recent graduates. Boyd & Elliso (2008) defined social networking sites as web-based services that allow individuals to construct their profiles within a bounded system, to articulate a list of other users, with whom they want to share a connection and to view and exhibit their list of connections within the system. The uniqueness of social networking sites is that it allows individuals to meet strangers and to get in touch with existing friend groups. With a variety features provided by SNSs, users can build up their profiles and decide whether to make it visible to public or only specific groups of friends. Most SNSs provide opportunities to view friend lists, to leave a message on their friends' profiles, to share photos, VDOs or web links. The most popular social networking sites include Facebook, MySpace, LinkedIn and Twitter. Among these, Facebook has the greatest number of users. By 2011, it was reported to have 500 million users around the world (Facebook, 2011); during Twitter has around 106 million users and mySpace 100 million users (Social networking watch, 2011). Because of its dominance in the field, this article will focus on Facebook, but the arguments also apply to the other social networking sites.

Facebook's main purpose is to help people communicate efficiently with friends, family and co-workers. Facebook users can create a personal profile and upload desired information such as personal photos, contact information, personal interest and status updates. Users can search for other users and add them into their friend lists. They may also join common interest user groups and like page to share interest, political view, sexual orientation, religion beliefs and any number of others personal



interest (Ellison et al., 2007). Lots of information is disclosed and shared through Facebook. Based on this ground, organizations are using Facebook and other SNSs to collect comprehensive information about job candidates.

In general, a recruiting process consists of different activities. Organization's first task is to identify and to attract potential employees (job candidates). Once the organizations have enough numbers of applicants or when the pool of qualified candidates is established, organizations will go to the next step: a screening and selecting process. This refers to the activity of collecting and evaluating the information about an applicant in order to extend an offer of employment (Gatewood et al., 2008). The recruiter organizations may use several selection devices such as the application form, interview, employment test, assessment centre and background check.

Traditional background check generally focuses on resume accuracy, criminal history, credit history, drug screening, educational backgrounds and reference verification. The aim of background check is to verify information and to determine the "fit" between the job and applicants. Theoretically, recruiter organizations will only take the information and the observation related to the job as the basis to predict the employee job performance in the future (Caers & Castelyns, 2010). As the background checks conducted through third party institutions can be costly, mainly because of the time and effort necessary to explore and verify every comprehensive details of a person, organizations tend to conduct applicant background check by themselves through Internet, by using social networking sites, as this provides an inexpensive and quick way to gather the basic information about job candidates. Starting with a search engine such as Google or Yahoo, recruiter organizations can link to job candidates' profiles, as some SNSs allow the Internet search engines to search the name of its users and make the profiles available for public. Recent surveys by various entities have confirmed the growing trend of employers conducting online check using SNSs. A study carried by CareerBuilder.com in 2006 revealed that 25% of hiring managers have conducted Internet searches by using search engines such as Google and 12% have looked at job candidates' profiles in SNSs (CareerBuilder, 2006). A survey of Society of Human Resource Management indicated that 50% of human



resource professionals ran an Internet search (Google, Yahoo), 15% checked SNSs and 40% of those who do not currently check said, they were likely to check within a year (Ziedner, 2007). The same trend was cited in Vault's Social Networking Survey, 44% of employers reported checking SNSs for job candidates' information (Vault.com, 2009). The survey from Jackson Lewis (LLP Survey) focused on New York employers as well as Global Interviewing Perceptions Survey in the United Kingdom reported that more HR professionals had searched on SNSs to gain additional information (HRtools.com, 2008, Peacock, 2009).

On one hand, recruiter organizations can use peripheral information provided in SNSs to draw a quick character picture of a job candidate. This helps organizations make an assumption about the personality of job candidates, to predict how they would work in the organization and to determine whether he/she fits in the organization (Rynes & Barber, 1991, Braddy et al., 2003). But on the other hand, information in SNSs could contribute a negative consequence, as this can affect the employment decision (Brandenburg, 2008). This statement was confirmed by a number of surveys. CareerBuilder.com reported 63% of employers rejected job candidates because of information founded in SNSs (CareerBuilder, 2006). And Global Interviewing Perceptions Survey indicated that 52% of global employers believed the information in SNSs impact their hiring decision (Peacock, 2009).

This negative consequence leads to a discussion whether it is legal to run online background checks without the permission of the person being screened and whether this complies with an ethical manner a business organization should have. The next sections will discuss this legal issue.

2. Legal issue related to online background check

Making an accurate hiring decision is extremely important for most employers. The cost associated with making a poor hiring decision could be enormous (Calvasina et al., 2008). Therefore organizations perform necessary tasks to protect themselves by mitigating risks through due diligence and exercising a distinguished degree of care when evaluating job candidates. Information provided in social networking sites are widely used by organizations as a screening tool for job applicants. But this



could be seen as infringement on personal right to privacy. More details about the right to privacy and the use of social media in employment background check will be explained in the following sections.

2.1 The right to privacy

The right to privacy has been recognized for several decades. Great philosophers, such as, Aristotle and John Locke have mentioned the right to privacy in their works (DeCew, 1997). However, the universal definition of privacy does not exist (Miller & Weckert, 2000). But there is a general belief that there is a natural right to have some information about oneself kept from others. Individuals have a natural right to be left alone and can control over knowledge about oneself (Introna & Pouloudi, 1999). The right to privacy has a close relation to human dignity, and in many countries it is regulated as a fundamental right in the constitution. For example, the Human Rights Act 1998 of the UK provides a person with the right to have one's private life respected (Jeffery, 2002). As well, the European Convention on Human Rights assures the right to personal privacy in Article 8 (Vigneau, 2002). As individuals' right to privacy are guaranteed in several ways, the users of social network sites have the option to carry out their privacy setting.

2.2 Privacy Setting in Facebook

Facebook provides privacy setting, in which users can control exactly who can access their profiles by including or excluding certain friends as well as who can search for them and how they can be contacted (Brandenburg, 2008). Facebook has granted privacy policy as followed:

"Facebook is about sharing information with others — friends and people in your networks — while providing you with controls that restrict other third parties from accessing your information. We allow you to choose the information you provide to friends and networks through Facebook. Our network architecture and your privacy settings allow you to make informed choices about who has access to your information. We do not provide contact information to third party marketers without your permission. We share your information with third parties only in limited circumstances where we believe such sharing is 1) reasonably necessary to offer the service, 2) legally required or, 3) permitted by you" (Facebook, 2011).



This privacy policy seems encompassing at the first glance. However, many users simply do not activate their privacy setting and even if they do, there is no 100% guarantee that this privacy setting can limit or block others from viewing their profile (Brandenburg, 2008). Third parties such as hiring organizations or employers can access job applicants' Facebook profiles in a variety of ways as followed.

2.3 Hiring organizations' access to Facebook profiles

The easiest way is an organization or HR professional signs up for an account and views the applicants' profile directly, if the profile has no access restriction. The organization can also use their current employees' Facebook account to search applicant's profiles, if they are in the same network, such as, the same school, college or hometown. Some organizations even hire current students who can access their peers' profile and effectively circumvent any privacy settings that a job candidate has set up to keep away the unwanted person from accessing their profiles. Possibly, organizations may access Facebook profiles by hacking into Facebook database. This seems complicated, but it may not be a hard task for many IT - specialists at most companies. By hacking, organizations would have access to any profiles they wish. It is also possible for a hiring organization to collect applicants' information through indirect means. For example, when an applicant's profile is restricted with privacy setting, organizations can access the profiles from applicant's Facebook friends, as some of these may not be well protected. Organizations can see what kind of friends an applicant has and eventually make an assumption about the personality of the job applicants.

These examples show that there are various ways in which hiring organization can access applicants Facebook profile and make decisions about applicants' character, which could have an impact on hiring decision. In order to determine whether the matter of fact that an unauthorized use of information provided in social network sited by organizations for hiring purposes constitute an invasion of privacy, it depends mostly on a reasonable expectation of privacy (Waldman, 2001). The next sections will provide extensive details about the expectation of privacy, which is the vital factor to determine whether individual's right to privacy is protected. Moreover, it will give an overview on workplace privacy orientation and laws in different countries.



3. Expectation of privacy

The expectation of privacy is a legal test which is crucial in defining the scope of the applicability of the privacy protections. Individuals receive no Fourth Amendment protection unless they can demonstrate that they have a reasonable expectation of privacy in the place that was searched or the property that was seized (US Constitution, 2011). There are two types of expectation of privacy; a subjective expectation of privacy which is an opinion of a person that a certain location or situation is private; and an objective, legitimate or reasonable expectation of privacy which is an expectation of privacy generally recognized by societies. As Facebook provides the users the control over the accessibility of information shared, and users can use privacy setting to block the unwanted person from viewing their information, it is likely to be that Facebook users believe their information posted in SNSs is secured. So they have expectation of privacy (Brandenburg, 2008). However, it is debatable whether this is a reasonable expectation of privacy. There is uncertainty whether a person retains a right to privacy and a reasonable expectation to privacy when he/she originally intended to keep the information private or share only to some specific persons, but the unintended recipients also got this information. Or in another case, when a person intends to disclose the information to specific third parties, whether this means the person waives his/her reasonable expectation of privacy; once the information is provided to some, it possibly means that it is accessible by all. The following court decisions provide the answer to these questions.

In the *Multimedia WMAZ, Inc. v. Kubach* case, in which Mr. Kubach, an HIV positive man agreed to be a guest for a report about HIV, but only under the condition that his identity was kept private and his image distorted to render it unrecognizable. Unfortunately, the distorted did not work and Mr. Kubach was recognised by television viewers above all his community. He sued a television station, but the television station claimed that the plaintiff (Mr. Kubach) had no reasonable expectation to privacy as to the fact that he was HIV positive because he has disclosed this information to family members, some friends and members of HIV supporting group; many people were aware of that fact. But the court determined that the plaintiff retained reasonable expectation of privacy, stating the plaintiff has expressed his illness to



some, because they cared about him and because they also had AIDS. And although Mr. Kubach did not tell his family and friends to keep this information confidential, it is to understand that Kubach's illness was not something they would discuss indiscriminately (*Multimedia WMAZ Inc. v. Kubach*, 443 S.E. 2d 491, Georgia Court Appeals 1994).

In *Sanders v. American Broadcasting Co.*, an ABC journalist obtained employment as a telephone psychic and used her hidden camera to record her conversations with her new co-workers, Sanders. After some part of this conversation was broadcasted on television, Sanders sued the undercover journalist. The journalist argued that Sander had no reasonable expectation of privacy because the co-workers who were in that area could overhear her conversations. But the court disagreed with this argument and stating that a person who reveals information about him or herself to some people may have the right to keep that information private from other unintended persons under the law of tort for the breach of privacy. The mere fact that a person can be seen by someone does not automatically mean that he or she should be legally forced to be seen by everyone (*Sanders v. American Brdcst. Co.*, 978 P. 2d 67, 72, California 1999).

But in some cases, the disclosure of information to third parties can violate the right to privacy; for example, in *Nader v. General Motors Corp.* In this case, Nadar, an author who published his bestseller, *Unsafe at Any Speed*, was threatened by GM in that it dug into his personal information and his past. Furthermore, the company interviewed Nader's friends and family, asking about his private life, his interest, religious beliefs, sexual orientation etc. under the false pretense that it was the background check for recruiting purposes. The court argued that the information already known to others could hardly be seen as private; therefore, Nader could not expect his right to privacy, even though he has shared this information only with some specific persons (*Nader v. Gen Motors Corp.*, 225 N.E. 2d 765, New York 1970).

From these cases, one can assume that there is no specific regulation which determine whether a plaintiff has a reasonable expectation of privacy. The number of persons to whom a plaintiff has shared the information cannot be used as a key factor to decide whether a plaintiff has an expectation of privacy. Being seen



by someone does not mean one should be seen by all, but at the same time, providing the information to someone can be interpreted as providing to all. It is difficult to know, how a court might judge the Facebook user's privacy claims against an employer who accesses the user's profile without permission (Brandenburg, 2008).

Some researchers have mentioned the right to privacy on social networking sites in their works. For example, Introna and Pouloudi (1999) stated that job applicants abandon their expectation of privacy to the information when they posted it on social networking sites because social networking is about sharing information to the public. Warren and Brandeis (1980) argued that a person's right to privacy ceases once the individual publishes the information or consents to its release. Similarly, these arguments were recently used by the New York Trail court, who ordered a defendant to grant a plaintiff an access to the former's social networking accounts, including deleted materials. In *Romano v. Steelcase, Inc.* case, Kathleen Romano brought a personal injury action against the defendant (Steelcase) claiming damages related to her loss of enjoyment of life following her injuries. As part of its defense, Steelcase asked the court for an order granting its access to plaintiff's current and historical Facebook and MySpace pages and related information upon the ground that the plaintiff (Romano) placed certain information on the social networking sites, regardless of the privacy settings Romano used in restricting access to such postings. The court reasoned that a review of the limited posting on Facebook and MySpace could lead to the disclosure of evidence, which the plaintiff tried to hide by using private setting. Additionally, the denying of the defendant's access to those private pages would infringe New York's liberal discovery policies. The court also considered plaintiff's argument about her right to privacy because she has used the privacy setting. However, it was held by the court that the plaintiff had no reasonable expectation of privacy in the content she posted on Facebook and MySpace, as the defendant's need for the information contained on the plaintiff's private Facebook and MySpace pages outweighed the right to privacy. And because neither Facebook nor MySpace guarantees absolute privacy, the court argued that the plaintiff has no legitimate reasonable expectation of privacy. As the result, the defendant was granted the right to explore the plaintiff's social networking sites (*Romano v. Steelcase Inc.*, 907 N.Y.S.2d 650, 2010).



Using this argument in the recruiting context, it is likely that employees have no reasonable expectation of privacy in the content posted to a social networking site, as SNSs provide insufficient protection of privacy and when the need in viewing SNSs profiles outweighing the right to privacy. Therefore, employers may commence an investigation on the employees' profiles on Facebook or other social networking sites because they could legally do so.

However, the cases mentioned above are based on the American constitution and law. The US courts have interpreted the existence of the right to privacy stemming from several constitutional amendments (Decew, 1997). But other countries may have different rules about what information is deemed private and public, and how the privacy in the workplace is regulated. The following section will provide an overview on some of the major differences in different countries in their regulations on workplace privacy.

4. Workplace privacy orientation and laws

4.1 Germany

In Germany, there is a mixture of laws that provide some workplace privacy and comply with the directive from European Commission (Directive 95/46/EC). Employers have the right to collect some personal data about employees but monitoring or surveillance of the employee without giving them a notice can only happen under specific circumstance. But generally the collection of personal data must be authorized by law or when a person consents (Reinhard, 2002). The Federal Data Protection Act (*Bundesdatenschutzgesetz, BDSG*) provides a framework regarding online background check. Employers can search for applicant's data online, if the data are used for employment-related purposes e.g. for hiring decisions or terminating the employment contract (Section 32 BDSG). However, collecting data from social networking sites could be seen as a violation of individual's right to privacy, when the privacy setting is implemented. Furthermore, background check in SNSs has to be complied with Anti-Discrimination Law (*Allgemeine Gleichbehandlungsgesetz, AGG*), which aims to provide an equal treatment for every job candidates. Employers are not allowed to search for intimate information of the job applicants because such information is not allowed to be asked in the interview. And the job decision has to be made without discrimination of age, sexual orientation, religious belief, ethic or age.



4.2 France

In France, there are three principles that guide workplace privacy, namely the principle of transparency that prior notice be provided to an employee before workplace surveillance or personal data is being process; the principle of proportionality which requires that the methods used to gather the information must be balanced to the depth or type of information needed; and the principle of relevance requires the employer to justify the need for the information. Information sought from job applicants and employees must aim exclusively at evaluating their professional abilities and relevant to the job (Vigneau, 2002).

4.3 Thailand

In Thailand, there are many sources of law that related to personal data protection. For example, the Official Information Act 1997 provides the principles and mechanisms to protect people's right to know and stimulate the free-flow of information between people and public administration, and regulate how the personal information is collected and used within state agencies or state enterprises (Privacy International, 2007). There are also specific requirements relating to personal data collection, such as the Financial Institutions Act, the Credit Information Business Operation Act, and the National Health Security Act. These set out additional obligations and provide a comprehensive framework for data protection, but these acts are applicable only within these industries, or to those who use such information. However, the Personal Data Protection Act is still at a very early stage (not yet enacted). The Act takes a general approach that a data controller may not collect use or disclose any personal data without the consent of the data owner, unless authorized by law. Additionally, the Act contains an outright prohibition on the collection of data relating to sexual conduct, criminal history, health, national origin, race, political opinion, religious beliefs, data that is detrimental, impairs one's reputation, or causes any sense of discrimination. Nevertheless, there is no specific regulation about the online background check conducted by employers, whether this complies with Personal Data Protection Act. But one can assume that as long as the information collected does not lead to discrimination of job applicant, the employers are allowed to do so. The next section will provide the implication for employers how to conduct

the online background check in order to minimize the legal risk of privacy right violating.

5. Implications for employers

There are many aspects to online background check in social networking sites, above all the right to privacy, the protection of personal data, and the discrimination aspect. Employers could, in some countries, legally conduct online background check, as these serve as a tool to prevent fraud, and other activities that may be detrimental to the employers or, to reduce the risk of failed hiring. Nevertheless, in some countries the area of background checks is new and unregulated. The court systems, as well as our federal, state and local laws, are lagging far behind technological advances. The search on information of job applicants without consent can be seen as unethical and this could lead to negative consequences, such as damage to the image of the organization or the lawsuit. Therefore, online background check has to be done with caution. Here is some guidance for online background check. Employers should:

1. Have a legitimate purpose – Employers should identify the purpose for conducting an online background check, and should inform the job applicants in advance.

2. Ask for consent – To avoid the violation of privacy, it is better to ask the job applicants for consent. Employers are on the safest legal ground if they ask the applicants, in writing, to consent to the background check. Employers should explain how the check will be conducted and how the data will be gathered. Also, they should ensure that the process is done confidentially.

3. Make sure that the inquired information is related to the job – The information searched from the online background check should be specific, factual and job related in content. Employers are not allowed to ask about health, disability or information about applicants' private life e.g. family planning, belief, sexual orientation etc., as these are not job related and are likely to lead to a discriminatory manner in hiring decision. Therefore, asking for or inquiring such information is prohibited by law in oral interviews and also online background check.

4. Ensure that the recruiting process is fair and the background check is applicable equally – Employers have to be consistent with background check. As with other recruiting tools, employers should not discriminate any applicants; therefore,



the background check has to be done equally and similarly with every job candidates. A record on how the recruiting process is conducted may be necessary, as this can increase the transparency of the recruiting process and helps job applicants to track back, why he or she is denied for an employment.

5. Not to rely on a single reference or information – It is important to keep in mind that there may be some inaccuracies of certain information provided on social networking sites, as some job candidates many have posted information that is false or wildly exaggerated, in an effort to be humorous and outstanding (Epstein, 2008).

6. Respect the privacy right of job applicants - Employers should not attempt to gain access to job applicants' Facebook profile when the privacy setting is used, or when it is not allowed to do so. As employees or job applicants have the right to privacy regarding personal matters, online background check has to be done with respect and should be complied with the law.

Conclusion

Information technology and Internet are widely adopted in business organizations and used in many business functions. Employers are using social networking sites to conduct online background check, which is on one hand, a useful tool for the employers in selecting the right job candidates for their organizations. However, the information provided on social networking sites could lead to a bias to the decision making and discrimination against job applicants. Furthermore, viewing job candidates' profiles without their consent (even though the profile is set as public) could be seen as an infringement of the right to privacy; it is unethical and could lead to negative consequences. Since the law in some countries may not cover the online background check and its privacy right issues; to avoid any legal risks, online backgrounds checks should be done with the consent of job applicants and have a legitimate purpose (job related). Employers should respect the right to privacy and should not discriminate any job applicants.



References

- Allgemeine Gleichbehandlungsgesetz (AGG), retrieved from
<http://dejure.org/gesetze/AGG>, on 8.05.2011.
- Boyd, D.M. & Elliso, N.B. (2008): Social network sites - Definition, history and scholarship, Journal of Computer Mediated Communication, Vol. 13, p. 210-230.
- Braddy, P.W., Meade, A.W. & Kroutalis, C.M. (2008): Online recruiting – The effects of organizational familiarity, website usability, and website attractiveness on viewers' impressions of organizations, Computer in Human Behavior, Vol. 24, Nr.6, p. 2992-3001
- Brandenburg, C. (2008): The newest way to screen job applications – A social networker's nightmare, Federal Communications Law Journal, Vol. 60, Nr. 3, p. 597-626.
- Bundesdatenschutzgesetz (BDSG), retrieved from
<http://dejure.org/gesetze/BDSG>, on 8.05.2011.
- Caers, R. & Castelyns, V. (2010): LinkedIn and Facebook in Belgium - The influences and biases of Social Network Sites in recruitment and selection procedures, Social Science Computer Review.
- Calvasina, G.E., Calvasina, R.V., Calvasina, E.J. (2008): Making more informed hiring decision – policy and practice issues for employers Journal of Legal, Ethical and Regulatory Issues, Vol. 11 (1).
- Careerbuilder.com, background check, retrieved from
<http://www.careerbuilder.com/Article/CB-719-Interview-Tips-Jobseekers-Beware-of-Background-Checks/>, on 8.05.2011.
- Careerbuilder.com, One-in-Five Employers Use Social Networking Sites, retrieved from *<http://www.careerbuilder.com/share/aboutus/pressreleasesdetail.aspx?id=pr459&sd=3%2F10%2F2008&ed=12%2F31%2F2008>*, on 8.05.2011.
- Decew, J.W. (1997): In pursuit of privacy – Law, ethics and the rise of technology, Cornell University Press.



- Ellison, N.B., Steinfield, C. & Lampe, C. (2007): The benefits of Facebook "friends" – Social capital and college students' use of online social network site, *Journal of Computer-mediated Communication*, Vol. 12, Iss. 4, p. 1143-1168.
- Epstein, D. (2008): Have I been googled? Character and fitness in the age of Google, Facebook and Youtube, *The Georgetown Journal of Legal Ethics*, Vol. 21 (3).
- Facebook, Press releases, retrieved from <http://www.facebook.com/press/info.php?statistics>, on 5.05.2011.
- Facebook, Privacy policy, retrieved from <http://www.facebook.com/policy.php>, on 10.06.2011.
- Gatewood, R.D., Feild, H.S. & Barrick, M. (2008): *Human Resource Selection*, Thompson.
- HRtools.com, Social networking survey results by one of Nation's largest employment law firms', retrieved from http://www.hrtools.com/legal_compliance/articles/social_networking_survey_results_released_by_one_of_nations_largest_employment_law_firms.aspx, on 5.05.2011.
- Introna, L.D. & Pouloudi (1999): Privacy in the information age – Stakeholders, interests and values, *Journal of Business Ethics*, Vol. 22 (1).
- Jeffery, M. (2002): Information technology and worker's privacy – The English Law, *Comparative Labor Law and Policy Journal*, Vol. 23(4).
- Miller, S. & Weckert, J. (2000): Privacy, the workplace and the internet, *Journal of Business Ethics*, Vol. 28 (3).
- Multimedia Wmaz, Inc. v. Kubach., 212 Ga. App. 707, 443 S.E.2d 491 (1994), retrieved from <http://georgia-court-appeals.vlex.com/vid/multimedia-wmaz-inc-v-kubach-20437432>, on 9.06.2011.
- Nader v. Gen Motors Corp., retrieved from <http://www.4lawschool.com/torts/nader.shtml>, on 9.06.2011.



- Official Information Act B.E. 2540, view online <http://www.thailawforum.com/database1/official-information-act.html>, on 9.06.2011.
- Peacock, L. (2009), Social networking sites used to check out job applicants, retrieved from Personnel today website: <http://www.personneltoday.com/articles/2009/03/17/49844/social-networking-sites-used-to-check-out-job-applicants.html>, on 5.05.2011.
- Privacy International, Constitutional privacy framework, retrieved from <https://www.privacyinternational.org/article/phr2006-kingdom-thailand>, on 9.06.2011.
- Rheinhard, H.J. (2002): Information technology and workers' privacy – The German Law, Comparative Labor Law and Policy Journal, Vol. 23(4).
- Romano v. Steelcase Inc., retrieved from http://www.ediscoverylawalert.com/uploads/file/2010_N_Y_Misc_LEXIS_4538Romano.pdf on 5.06.2011.
- Rynes, S.L. (1991): Recruitment, job choice, and post-hire consequences – A call for new research directions, in M. Dunnette, M. & Hough, L. (Eds.), Hand book of industrial/organizational psychology, p. 399-444.
- Sanders v. American Broadcasting Co., Filed 6/24/99, retrieved from <http://lw.bna.com/lw/19990713/s059692.htm>, on 5.06.2011.
- Social networking watch, MySpace's Decline Is Accelerating, retrieved from <http://www.socialnetworkingwatch.com/2011/03/myspaces-decline-is-accelerating.html>, on 5.05.2011.
- Society of Human Resource Survey, retrieved from <http://www.shrm.org/Research/SurveyFindings/Articles/Pages/ConductingReferenceBackgroundChecks.aspx>, on 5.05.2011.
- US Constitution, Amendment 4 - Search and Seizure, retrieved from <http://www.usconstitution.net/const.html#Am4>, on 5.06.2011.
- Vault.com, Social networking website survey, retrieved from <http://www.vault.com/surveys/social-networking/index.jsp>, on 7.05.2011.
- Vigau, C. (2002): Information technology and workers' privacy – The French law, Competitive Labor Law and Policy Journal, Vol. 23(4).



Waldman, M. (2001): Annotation – Expectation of privacy in Internet communication, American Law Report 5th.

Warren, S.D. & Brandeis, L.D. (1890): The right to privacy, Harvard Law Review, Vol. 4(5).

Ziedner, R. (2007): How deep can you probe?. HR Magazine, Vol. 52 (10).