PRE-EMPLOYMENT BACKGROUND CHECKS ON SOCIAL NETWORKING SITES - MAY YOUR BOSS BE WATCHING?

by

SEILI SUDER[*] [**]

The practice of using social networking sites (SNS) for pre-employment screening has become increasingly popular. Although using SNS as a hiring tool may prove to be a potentially promising source of applicants' information, it is also fraught with potential risks that uncover both legal and ethical challenges. The latter is also the reason why there are conflicting views about the practice both among the employers and employees as well as legal systems.

In this paper I first aim to compare the privacy approaches in the US and Europe to investigate whether a job applicant actually has a right to expect privacy on SNS, and then I will examine the practices in a set of European countries (Estonia, United Kingdom, Germany, Finland) to analyze under what conditions employers are allowed to carry out background checks on SNS and weather the employer may base their hiring decision on the information found from these public domains.

My analysis suggests that pre-employment background checks are generally considered to be acceptable in the US and also in Estonia; employers in the UK, Germany and Finland however, are not always allowed to investigate applicant's background on SNS and should thus not be able to base one's hiring decisions on the information found from SNS.

My analysis reveals that the countries and employers need to work towards clarifying privacy standards and policies that would take into account the context created by the new technologies.

---

[*] Faculty of Law, University of Tartu, Estonia. Contact: seili.suder@sm.ee

[**] Writing of this manuscript was supported by the project PUT44 financed by Estonian Scientific Agency.

KEYWORDS
Pre-employment Screening, Background Checks, Social Networking Site, Privacy

1. INTRODUCTION

Since their introduction social networking sites (SNS) such as Facebook have attracted millions of users who have integrated these sites into their daily lives. There are hundreds of SNS supporting a wide range of interests and practices. Most sites support the maintenance of pre-existing social networks, but others help strangers to connect based on their shared interests, political views, or activities (boyd & Ellison 2007).

In the recent years studies carried out in Estonia (Visamaa 2011; Ivask 2013) as well as other countries (PR Newswire 2012) suggest that employers are using social media channels, especially SNS more and more to employ and do background checks on employees. While the practice seems to be taken for granted as acceptable in the US, EU countries still weigh the possibilities and legal consequences of using SNS as a screening tool.

The growing popularity of using SNS for this reason is usually justified by the fact that such an approach is quick and inexpensive and enables to draw conclusions about applicant's character. Studies indicate that this practice is variable among employers. Interviews carried out with employers (n=10) working in the service sector organizations in Estonia reveal that although Facebook, Google and other online platforms were actively used by all of the interviewees for background checks, the practices and timing of these checks differed between organizations (Ivask 2013).

Furthermore, the results of recent studies indicate that such background checks affect applicants chance to get hired. According to the findings of a survey carried out by CareerBuilder, 29 per cent of US employers hired an applicant due to the background information received from SNS, whereas 34 per cent of the employers admitted not hiring an applicant due to detrimental information found on SNS (PR Newswire 2012).

Studies carried out among employees, on the other hand, show that these background checks are considered to be unacceptable as they may lead to premature conclusions about applicants' personality and skills. For instance findings from a study carried out in the US indicate that 56 per cent of the sample considered it "somewhat" or "very inappropriate" for em-

ployers to seek information about candidates using SNS (Abril, Levin & Riego 2012).

Practice of using SNS as a hiring tool has also become a growing ethical and legal concern for courts and lawmakers both in the US and Europe. The personal information a user posts online, combined with data outlining the users actions and interactions with other people, can create a rich profile of that person's interests and activities. Personal data published on SNS can be used by third parties for a wide variety of purposes, including loss of employment opportunities (European Commission 2009).

All of the above shows that there are conflicting views about the practice both among the employers and employees. The aim of this paper is twofold. On the first part of the paper I will compare the privacy approaches both in the US and EU in order to investigate whether an applicant actually has a right to expect privacy on SNS. In the second part of the paper, I will examine the practices in a set of EU countries (Estonia, United Kingdom, Germany, Finland) to analyze under what conditions employers are allowed to carry out background checks on SNS and weather the employer may base its hiring decision on the information found from these public domains.

2.1 APPLICANTS' RIGHT TO PRIVACY ON SNS

SNS have made private information become easily accessible to the general public and not only to one's "ideal audience" (Marwick & boyd 2010) i.e. family and friends, but also to "nightmare readers" (ibid.) i.e. employers, recruiters, clients etc. The information on SNS may provide evidence related to the veracity of information presented on an applicant's CV and give access to detailed information about future employees making it easier to draw conclusions about the applicant's character (Brown & Vaughn 2011). Do applicants actually have a right to expect privacy on public forums like SNS?

Paradoxically there is no single definition of privacy but the right itself is universally recognized and declared in numerous constitutions and international instruments. What is included in that right, however, is often debatable as there are conflicting interpretations of which types of privacy warrant legal recognition and protection (Lasprogata, King & Pillay 2004). The European Court of Human Rights for example has stated numerous times that private life is a broad term not susceptible to exhaustive definition (Niemietz vs Germany 1992). One of the possible definitions of 'privacy' has

been provided by Warren and Brandeis who argued that humans have a natural right to be left alone to determine to what extent his thoughts and emotions shall be communicated to others (Warren & Brandeis 1890). Privacy has also been described as a freedom from judgments of others (Introna & Pouloudi 1999). Our current understanding of informational privacy is based to some extent on how an individual relates to and controls access to information about themselves (Robinson et al. 2009).

Usually the more intimate something feels to a person, the more it is considered a private issue that will only be shared with someone close (Trepte & Reinecke 2011, p.47). For example, the more applicants disclose on SNS, the more they risk what they themselves consider breaches of their privacy (ibid. p 3). Still, even if the information that an individual places on SNS is personal or protected information, many are convinced that a person waives an expectation of privacy to that information when one posts it on a SNS (Introna & Pouloudi 1999). The latter idea is also dominating among employers. For instance, a case-study among service sector employers in Estonia reveals that employers were convinced that information on SNS is publicly available and may hence be browsed by them (Ivask 2013).

I argue that compromising applicants' privacy on SNS, however, may result in various types of harm. According to Van der Hoeven and Weckert (2008) harm that may arise as a result of the compromise of privacy protections is information injustice i.e. information presented in one context is used in another. It is logical to suggest that employers must consider the role of context when investigating applicants' background using SNS. However, the interviews with employers indicate that they rarely see any ethical dilemmas when conducting such checks (Ivask 2013).

Negative information conveyed through the applicant's personal profile may not be considered in the proper context, and could therefore result in a hasty rejection decision (Brown & Vaughn 2011, p. 220-221). The interviews with Estonian employers indicate that the information found from SNS might in some occasions truly affect the applicant's ability of getting hired (Ivask 2013).

Furthermore, SNS represent an extensive source of information that may be able to reveal untapped job-relevant (and job-irrelevant) applicant characteristics. For example, internet search might reveal job-irrelevant information about applicant's political activities, national origin, religion and other information that might not arise during a traditional background check. The

use of Internet screening for selection may therefore lead to discrimination (Davison et al. 2012, p. 2). The findings of the interviews with the employers, for instance, suggest that applicants' photos, friends' lists, comments and "likes" are most often scrutinized to gain some additional knowledge of the applicant (Ivask 2013).

In addition, information on SNS may vary considerably, which makes comparison between applicants unreliable. Shared information on SNS might be distorted by social desirability or high levels of self-monitoring and SNS may contain inaccurate information. The interviewed employers from Estonia, however, believed that the information they find from online environment is trustworthy (Ivask 2013).

When analyzing the privacy expectations of an applicant I tend to agree that a person waives his expectation of privacy to information that is posted on SNS. As public information is not considered private and therefore it is hard to argue otherwise. As the information on SNS is publicly searchable an applicant should not have a right to privacy on SNS. Still when compromising privacy protection the harm that may arise when using SNS as a hiring tool is alarming. Due to the available information online employers are often able to investigate and monitor various pieces of information that are out of context, inaccurate, irrelevant and unreliable.

To analyze the matter further in the next sections of the paper I compare the privacy protection of applicants both in Europe and the US.

2.2 PRIVACY PROTECTION OF APPLICANTS IN THE US

In the US, the right to privacy is an individual right that can be exchanged for other rights and privileges, including those obtained in an employment relationship. Since privacy belongs to the individual, it may be traded away by the individual in exchange for something of commensurate value, such as a job (Lasprogata, King & Pillay 2004). So while most countries in Europe explicitly recognize basic privacy rights in their constitutions and have adopted general data protection laws, the US Constitution does not provide protection for employee privacy in private sector workplaces (ibid).

In the US employers are allowed to investigate the private lives of applicants and can also do so using SNS. According to Warren and Brandeis the right to privacy ceases upon the publication of the facts by the individual, or with ones consent (Warren & Brandeis 1890). US courts have already expressed a disinclination to find rights to privacy in online information. In-

ternet postings are not considered private since they are often available to the general public (Sprague 2011). Furthermore, if an employer discovers negative information about the job applicant using SNS, but decides to ignore the information and hire the individual anyway, then the employer could be sued for negligent hiring, if the employee later harms a third party (Davison et al. 2012, p. 8).

But as the discussion of privacy rights expands in the US we also encounter different attitudes in this matter. For example the US Supreme Court has analyzed the privacy expectations of an employee in the context of a new technology (text messages). The court emphasized that modern communications technology and its role in a society were still evolving. In fact, in their decision the court stated that it is difficult for them to predict how employees' privacy expectations will be shaped by those changes or the degree to which society will be prepared to recognize those expectations as reasonable. As the Court explained the more pervasive and essential or necessary an electronic tool becomes for an individual's self-expression or identification, the stronger is the case for an expectation of privacy (Supreme Court of the United States 2010).

2.3 PRIVACY PROTECTION OF APPLICANTS IN THE EU

In Europe the right to privacy and data protection are two distinct human rights recognized in numerous international (e.g. the Charter of Fundamental Rights of the European Union) and national instruments. In Europe the right to privacy is bound with human dignity. Human dignity is not generated by the individual, but is instead created by one's community and bestowed upon the individual. It cannot therefore be exchanged for other rights as seen in the US (Lasprogata, King & Pillay 2004).

With the evolution of new computer technology, the focus in recent years has been on the right to informational privacy. The main legal instrument regulating data protection in European Union today is the directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (hereafter directive).

Processing personal data for employment purposes falls within the basic framework of the directive, but there are no specific rules pertaining to the personal data of applicants. Directive contains an exhaustive and restrictive list of grounds for making data processing legitimate. For example according to article 7 (b) processing is lawful if it is necessary in order to enter into

a contract requested by the data subject, e.g. processing of data relating to an applicant.

According to article 6 of the directive, all processing (e.g. collection, storage) of personal data must comply with the principles related to data quality such as fairness, proportionality and relevance. In addition, the general obligations that only adequate, relevant and non-excessive data can be processed.

One of the goals of the directive is to make data processing more transparent to data subjects. Therefore according to article 11 the applicant has the right to be informed that data processing is taking place in case the data have not been obtained directly from the candidate himself (e.g. data are collected using SNS). The directive also envisages the right to access, correct and erase the data, but does not grant the data subject a general right to prevent a data controller from processing personal data.

I argue that the directive is unclear when analyzing what happens if personal information is available on SNS. According to the directive, all processing of personal data must comply with the principles related to data quality. Unfortunately it is ambiguous how to guarantee the fulfillment of these principles when information is collected from public domains.

We also have to take into consideration that the framework directive allows Member States to implement necessary measures while taking into account local traditions and sensitivities.[1] Therefore regardless of the directive, EU member states have different laws and practices covering applicant privacy rights. Some examples of counties are discussed in the next section.

3. EMPLOYERS' RIGHT TO USE SNS AS A HIRING TOOL IN ESTONIA, UNITED KINGDOM, GERMANY AND FINLAND

As previously described, the situation if and to what extent an employer may monitor applicants' SNS in EU is ambiguous and varies among countries. Most countries do not have a specific regulation that previses if and under what conditions an employer may use new communication technology to monitor applicants. Still it seems that in most cases privacy protection does not extend to publicly available data, such as SNS.

[1] In 2012, the European Commission proposed an overhaul of the existing legislative framework on the protection of personal data. New draft regulation does not further clarify the matters analyzed in this article. Still the regulation introduces for example the obligation on controllers to provide transparent and easily accessible policies with regard to the processing of personal data.

One example among countries that do not restrict employers' right to monitor applicants' SNS is Estonia as it does not have a specific regulation concerning data processing by employer. General data processing rules, which apply also in employment relationship, are regulated in the Personal Data Protection Act (DPA) (Riigiteataja 2007). However according to § 11 of DPA most of the act does not apply to the processing of personal data if a data subject has disclosed it (e.g disclosed data on SNS).

According to § 15(1) of DPA the employer must inform the applicant about data collection if the source of applicants' personal data is any other than the data subject oneself. Applicant has the right to demand the correction of data and that employer discontinues processing and deletes the data (DPA § 21(1); § 11(4)). According to the guidelines issued by Estonian Data Protection Inspectorate if the employer did not hire an applicant due to information found on SNS, the employer has the right to retain personal data till the applicant has the right to contest the decision, even in cases where the applicant has demanded the employer to discontinue searching data from SNS (Estonian Data Protection Inspectorate 2010). This right however is not explicitly regulated in the law and therefore enables different interpretations. Furthermore as only limited paragraphs in the DPA regulate the processing of disclosed data, it is very doubtful whether the data protection principles, regulated in § 6 of DPA, apply when employer investigates data from SNS.

Considering the above, it is possible to argue that in Estonia employers have the right to use SNS to get further information about applicants and may also base their hiring decision on the information found online. Employers' main obligation is to inform the applicant about data collection. It is questionable whether data protection principles have to be applied if data is collected from SNS.

Some European countries, such as the UK, Germany and Finland, however, restrict employer's right to monitor applicants' social media profile.

For instance, the primary legislation in the UK that regulates the holding of an individual's personal data by companies and regulates the processing of personal information of individual is the Data Protection Act (1998) which does not contain specific regulations on data collection during recruitment.

Guided by the data protection principles enacted in the act (schedule 1) the Information Commissioner has issued guidelines that explain informa-

tion gathering in the course of recruitment. The guide differentiates "verification" and "vetting". Verification covers the process of checking that details supplied by applicants are accurate. Vetting covers the employer actively making its own enquiries from other information sources. According to the guidelines employers may only use vetting where there are particular and significant risks involved to the employer, clients etc and where there is no less intrusive practicable alternative. Employers should inform applicants about vetting and carry it out at late stage in the recruitment process (Information Commissioner's Office).

Hence, the UK Data Protection Act does not prevent employers from using SNS during recruitment process but employers are strongly recommended to view applicant's SNS only when the employer faces particular risks and has notified the applicant. When SNS is used to screen applicants, employers must respect data protection principles and are urged to seek information from relevant sources and ensure that the extent and nature of information sought is justified.

Similarly to the UK, there are no detailed statutory regulations on data collection during the hiring process in Germany. Still statutory constraints with regard to the acquisition and storage of personal data are regulated in Federal Data Protection Act (Die Bundesbeauftragte … 2003). The Act allows employers to collect, process and use applicant's personal data for employment-related purposes where necessary for hiring decisions (section 32). When background checks are being carried out, the principle of direct acquisition of data via the applicant takes priority (Wisskirchen 2011).

Pursuant to the Act, collecting personal data from the internet is allowed if the data is accessible to the general public, unless the data subject has a clear and overriding legitimate interest in ruling out the possibility of processing (sections 28, 32). So data collection from applicant is unlawful if protectable interests of the applicant outweigh the interest of the employer. Therefore it is argued that data that is posted by the applicant on SNS like Facebook may not readily be collected and stored (Wisskirchen 2011).

The German Government is working on a draft law on special rules for employee data protection. Still a final decision on such new legislation is yet to be taken. One of the key issues covered in the draft is data collection in the recruitment process. According to the draft SNS that are used for electronic communication (e.g. Facebook) may not be used for research,

except for SNS that exist to represent the professional qualifications of their members (e.g. LinkedIn) (Out-Law.Com 2010).

There are also other countries in Europe that prioritize employees' rights to privacy protection when gathering information online. In Finland the Act on the Protection of Privacy in Working Life 759/2004 (Finlex 2004) expands employee privacy rights. According to the act employer shall collect personal data about the employee primarily from the employee himself. In order to collect personal data from elsewhere, the employer must obtain the consent of the employee (section 4(1)). Based on this regulation Finland's Data Protection Ombudsman ruled a decision that employers cannot use Internet search engines, such as Google, to obtain background information on job candidates (Kennedy & Macko 2009).

4. CONCLUSIONS

New forms of technology and communication (e.g. SNS) are changing our expectations of privacy. The challenge now for the lawmakers and the courts both in Europe and the US is the need to continuously monitor these changes and balance company's needs against individual rights and freedoms. In this article I have tried to demonstrate that although using SNS as a hiring tool provides a potentially promising source of applicants' information, it is also fraught with potential risks that uncover both legal and ethical challenges.

Online services, such as SNS, contribute to the distribution of knowledge and enable people to express themselves. But these useful communication tools have also transformed to an information base used by many unexpected eyes. Undoubtedly the recruitment and selection process necessarily involves collecting and using information about applicants. But we have to takes into consideration that when employer uses SNS to monitor applicants' background, much of personal information is revealed. Employers are therefore increasingly collecting data about the applicant that goes beyond their professional background.

We could argue that an applicant has the right to protect ones privacy by choosing a secure SNS with good privacy settings. Presently the users need to be digitally literate in order to even grave for any privacy settings not to mention make use of them. However, privacy policies of SNS should give an adequate warning to all their users of how their data is accessible to others, so that even the ones with less ICT skills and knowledge are in advance

warned by the possible consequences of data distribution and therefore have to take into consideration intrusions into their private sphere. Unfortunately there is a substantial diversity in the amount of privacy control offered by SNS and almost all policies are difficult for the ordinary person to understand due to confusing legal jargon. But most importantly when choosing a SNS the privacy settings are rarely a decisive feature.

When analyzing the privacy protection guaranteed by law, it is visible that the extent and range of privacy varies considerably among countries and is a complex notion. In the US applicants do not enjoy privacy protection when communicating on SNS. Still the discussion in this matter is ongoing and a judgment from US Supreme Court enables us to argue that in the future when new technologies become the norm of everyday life, the law may have to respond accordingly. In EU according to the directive, all processing of personal data must comply with the principles related to data quality. Unfortunately it is ambiguous how to guarantee the fulfillment of these principles when information is collected from public domains.

I tend to agree that a person waives his expectation of privacy to information that is posted on SNS. As public information is not considered private, it is hard to argue otherwise. Still when compromising privacy protection the harm that may arise when using SNS as a hiring tool is alarming and the interference into personal space can be remarkable. Due to the available information online employers are often able to investigate and monitor various pieces of information that are out of context, inaccurate, irrelevant and unreliable.

It seems that the debate in the US and developments in some European countries show an emerging trend towards protecting personal electronic media accounts. These new directions push the boundaries between the notions of private and public.

My analysis suggests that there are countries (e.g. Estonia) where employers have the right to use SNS to get further information about applicants and their hiring decisions may also be based on the information found online. Although Estonian employers' need to inform the applicant about data collection, it is questionable whether data protection principles have to be applied if data is collected from SNS. In fact, the analysis of Estonian practices suggests that information found on SNS is seen as available on a public domain and can be therefore used for obtaining specific information or be as a means of general intelligence gathering.

The examples from the UK, Germany and Finland, however, demonstrate that an employer is not always allowed to investigate applicant's background using SNS and should not be able to base ones hiring decisions on the information found from SNS.

In the legal point of view we need to recognize that there is a balance to be struck between legitimate interests of the employer and the rights of the individual. On the one hand, employers should not place reliance on information collected from unreliable sources such as SNS. On the other hand, it is also important to note that employers may have compelling business reasons to screen applicants' online activities.

To extract the most out of the current directive, I propose we seek agreement on efficient enforcement of applicants' rights and therefore encourage countries and employers to work towards clarifying privacy standards and policies that take into account new technologies.

REFERENCES

Abril, P. S., Levin, A. & Riego A. D. 2012, 'Blurred Boundaries: Social Media Privacy and the Twenty-First-Century Employee'. *American Business Law Journal*, vol. 49, no. 1, pp. 63-124.

boyd, d.n. & Ellison, N. B. 2007, 'Social Network Sites: Definition, History, and Scholarship', *Journal of Computer Mediated Education*, vol. 13, no. 1, pp. 210-230.

Brown, V. & Vaughn, E. 2011, 'The Writing on the (Facebook) Wall: The Use of Social Networking Sites in Hiring Decisions', *Journal of Business and Psychology*, vol. 26, no. 2, pp. 219-225.

Davison, H. K., Maraist, C.C., Hamilton, R. H. & Bing, M.N. 2012, 'To Screen or Not to Screen? Using the Internet for Selection Decisions', Employee Responsibilities and Rights Journal, vol. 24, no. 1, pp. 1-21.

Die Bundesbeauftragte für den Datenschutz und die Informationsfreiheit 2003, *Federal Data Protection Act* www.bfdi.bund.de/EN/DataProtectionActs/Artikel/BDSG_idFv01092009.pdf?__blob=publicationFile [May 10 2014].

Estonian Data Protection Inspectorate 2010, *Isikuandmete töötlemine töösuhetes [Processing of Personal Data in Employment Relationship]* https://www.aki.ee/et/juhised/isikuandmete-tootlemine-toosuhetes [Accessed May 10 2014].

Eur-lex 1995, *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, Official Journal L 281, pp 31–50 http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML [Accessed May 10 2014].

European Commission 2009, *Article 29 Data Protection Working Party. Opinion 5/2009 on online social networking* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2009/wp163_en.pdf [Accessed Nov 25 2013].

Finlex 2004, *Laki yksityisyyden suojasta työelämässä 759/2004 [The Act on the Protection of Privacy in Working Life 759/2004]* http://www.finlex.fi/fi/laki/ajantasa/2004/20040759 [Accessed Dec 01 2013].

Hoven, J.vd. & Weckert, J. (eds) 2008, *Information Technology and Moral Philosophy*, Cambridge University Press, New York.

Information Commissioner's Office, *The Employment Practices Code* http://www.ico.org.uk/for_organisations/data_protection/topic_guides/employment [Accessed May 10 2014].

Introna, L. D. & Pouloudi, A. 1999, 'Privacy in the information age: Stakeholders, interests and values', *Journal of Business Ethics*, vol. 22, no.1, pp. 27-38.

Ivask, E.-L. 2013, *The Use of Facebook as Evaluation Method for Job Candidates in Service Sector Organizations*, Bachelor Thesis, University of Tartu, Tartu.

Kennedy, N. & Macko. M. 2009, 'Social Networking Privacy and Its Effects on Employment Opportunities', *Human Capital institute* http://www.hci.org/lib/social-networking-privacy-and-its-effects-employment-opportunities [Accessed Dec 01.2013].

Lasprogata, G., King, N.J. & 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', *Stanford Technology Law Review*, vol. 4, pp. 1-46.

Legislation.gov.uk 1998, *Data Protection Act* http://www.legislation.gov-.uk/ukpga/1998/29/schedule/1 [Accessed Nov.19.2013].

Marwick, E. & boyd, d.m. 2010, ''I tweet honestly, I tweet passionately'': Twitter users, context collapse, and the imagined audience', *New Media & Society*, vol. 13, no.1, pp.114-133.

Niemietz vs Germany 1992, European Court of Human Rights, no 13710/88.

Out-Law.Com 2010, *German law bans Facebook research for hiring decisions* http://www.out-law.com/page-11336 [Accessed Nov 26 2013].

PR Newswire 2012, *Thirty-Seven Percent of Companies Use Social Networks to Research Potential Job Candidates, According to New CareerBuilder Survey* http://www.prnewswire.com/news-releases/thirty-seven-percent-of-companies-use-social-networks-to-research-potential-job-candidates-according-to-new-careerbuilder-survey-147885445.html [Accessed Nov 22 2013].

Riigiteataja 2007, *Isikuandmete kaitse seadus [Personal Data Protection Act]* https://www.riigiteataja.ee/en/eli/512112013011/consolide [Accessed May 10 2014].

Robinson, N., Graux, H., Botterman, M. & Valer, L. 2009, Review of the European Data Protection Directive, *Information Commissioner's Office* http://ico.org.uk/~/media/documents/library/data_protection/detailed_specialist_guides/review_of_eu_dp_directive.ashx [Accessed May 10 2014].

Sprague, R. 2011, 'Invasion of the Social Networks: Blurring the Line between Personal Life and the Employment Relationship', *University of Louisville Law Review*, vol 50.

Supreme Court of the United States 2010, City of Ontario, California et al. vs Quon et al., no. 08–1332 http://www.supremecourt.gov/opinions/09pdf/08-1332.pdf [Accessed Dec 12 2013].

Trepte, S. & Reinecke, L. (eds) 2011, *Privacy Online. Perspectives on Privacy and Self Disclosure in the Social Web*, Springer, Berlin.

Visamaa, K. 2011, *Veebipõhiste sotsiaalvõrgustike kasutamine töötajate värbamisel* [*The use of social networking sites in recruitment]*, Bachelor thesis. University of Tartu, Tartu.

Warren, S. D. & Brandeis, L. D. 1890, 'The Right to Privacy', *Harvard Law Review*, vol. 4, no. 5, pp. 193-220.

Wisskirchen. G. 2011, 'Background Checks in Europe', *Who'sWhoLegal* http://whoswholegal.com/news/features/article/29116/background-checks-europe/ [Accessed Nov 26 2013].