iS
CHANNEL

Privacy, Social Network Theory and Patterns of Information Revelation on LinkedIn

Marta Stelmaszak
MSc Management of Information Systems and Innovation (2013/2014)
Department of Management
London School of Economics and Political Science

KEYWORDS

Online Social Networks
Social Network Theory
Privacy
Information Revelation
LinkedIn

ABSTRACT

Online social networks and privacy are often discussed in relation to Facebook or other similar predominantly social platforms (e.g. Friendster). LinkedIn, despite many public concerns about privacy, rarely is the scope of research, though privacy breaches have been identified coming from other users, the service provider and third-party applications. The scope of this paper is to analyse privacy aspects on LinkedIn in relation to potential risks coming from other users through the application of the social network theory and the analysis of patterns of information revelation on LinkedIn. Following a detailed analysis of LinkedIn profiles and information revealed to different degree of connections, a range of findings is presented, including the increase in polarisation of connections, a substantial increase in the number of weak ties, an unprecedented number of connections, as well as potential risks arising from the degree of identifiability, type of information revealed and visibility of information on LinkedIn.

Introduction

"LinkedIn has slipped under the radar when it comes to privacy controls and transparency (…). Everyone points to Google, Apple and Facebook and pretty much stops there." (Veldt, 2013)

LinkedIn, an online social network (OSN) for professionals, was created in 2002 by Reid Hoffman to allow the creation of personal brands and identification online (Lacter, 2009). In 2014, the network boasts over 277,000,000 registered members (LinkedIn, 2014). Though mainly designed to facilitate professional networking, LinkedIn invites members to add professionally-relevant information about themselves, such as education, skills, present and past employment, as well as to share updates of activity. In other words, upon signing to this OSN members are assigned personal profiles which they are encouraged to fill out with details of their professional identities and then connect with other members with whom they have something in common. Due to the purpose of the network, as well as the nature of information shared, LinkedIn has not been as closely scrutinised as other OSNs, such as Facebook, in terms of user privacy and information transparency.

It seems to be widely accepted by members that information shared on this OSN is by default visible and its purpose is to attract potential connections or job prospects, unlike on Facebook. Though privacy concerns on LinkedIn may not mainly cover the type or nature of information revealed, they are present, often causing uproar among members and in nationwide media. In 2014, the most recent controversy surrounded third-party web browser plug-in software causing unwanted exposure of LinkedIn email addresses leading to privacy issues (BBC, 2014). In 2013, over 5,000 LinkedIn members signed a petition to LinkedIn to request a blocking function preventing unwanted individuals from viewing profiles due to stalking incidents (Change.org, 2013). Introduced in 2013 and quickly abandoned after a severe public reaction, the Intro function in iOS Mail is believed to have intercepted emails, added HTML to pull in extra information from LinkedIn and displayed it without users' permission (Sherman, 2013).

In 2010, the founder of LinkedIn himself caused a controversy after claiming at Davos Annual Meeting that "privacy is for old people" (YouTube, 2010). Many commentators concluded that such an attitude should cause concern over how LinkedIn approaches privacy in general (Cendella, 2011; Cavoukian, 2011).

This paper aims to examine the issues of privacy on LinkedIn in the light of social network theory (SNT) and patterns of information revelation (IR). In general, privacy breaches on OSNs may originate from service providers, from other users or third-party apps (Gao et al., 2011). This paper concentrates on analysing how the design of LinkedIn as an OSN impacts IR to other users in the light of SNT. Further, the paper

Corresponding Author
Email Address: M.Stelmaszak1@lse.ac.uk (M. Stelmaszak)

analyses what degree of information revelation and control over privacy is allowed on LinkedIn and to what extent it is used by members.

The first part of this paper provides a review of literature on key themes concerning this subject, including privacy and privacy breaches on OSNs, social networking searching, as well as social network theory. In the second part the paper outlines two main theoretical frameworks used to analyse the issue of privacy on LinkedIn, namely the privacy aspect of social network theory and patterns of information revelation. The third part of the paper consists of an empirical study of 15 profiles of LinkedIn members. The results of the study are presented and analysed, followed by a summary of findings.

Literature Review

Privacy and Privacy Breaches on OSNs

The research in privacy and privacy risks on OSNs has gained momentum with the development of Facebook and Twitter. One of the main topics in this body of literature aims at defining privacy in the context of OSNs, as researchers believe that current definitions of privacy may not reflect new settings and challenges (Tomlinson et al., 2010). Therefore authors analysing privacy on OSNs often refer to more traditional definitions of privacy and apply them to the online world.

A group of researchers argues that privacy can be seen as control of the access to self (referring to Warren and Brandeis, 1890; Altman, 1975; DeCew, 1997; Solove, 2006; Houghton and Joinson, 2010). Due to the lack of a unified and simple definition of privacy, some authors (Tomlinson, Yau, MacDonald, 2010) analyse privacy on OSNs following developed dimensions of privacy (such as Westin, 1967; Marshall, 1972, 1974; Pedersen, 1979; Burgoon et al., 1989).

Some authors (Houghton and Joinson, 2010) suggest that within the context of OSNs, privacy can be defined as "the claim of individuals, groups, or institutions to determine for themselves when, how and to what extent information about them is communicated to others" (Westin, 1967: 7). This stream of literature provides a thorough and acceptable definition of privacy for the purposes of this paper reflecting the purpose and mechanics behind LinkedIn.

Social Network Searching

Another source of literature relevant to the topic to provide the understanding of the use and type of information revealed on LinkedIn stems from the study of social network searching. As OSNs can be defined as platforms allowing individuals to "construct a public or semi-public profile within a bounded system, articulate a list of other users with whom they share a connection and view and transverse their list of connections and those made by others within the system, OSNs allow for increased benefits and threats arising from searchability" (Boyd & Ellison, 2007, p. 211).

Some authors argue that the development of OSNs "added a new dimension to the way that organisations search or investigate people" (Qi & Edgar-Nevill, 2011: 74). A study quoted in the paper, conducted by CareerBuilder.com in June 2009 suggests that more than 45% of managers who participated in the survey used ONSs to seek information on job candidates (Haefner, 2009). It is claimed that users' sharing a variety of information on OSNs raises concerns about organisations' access to personally identifiable data (Qi & Edgar-Nevill, 2011).

The stream of research in human resources on using social media for recruitment cannot be ignored, as it often aims at explaining why certain pieces of information are revealed by OSNs members. Some researchers analyse the biases of OSNs on the recruitment and selection procedures (Caers and Castelyns, 2010). In this context, the study conducted by the authors reveal that the majority of active LinkedIn members deem the network suited to be informed on friends' career developments (85.1%), find updates on other organisations (57.8%) and make professional connections (47%) (Caers and Castelyns, 2014: 442).

Social Network Theory

A large and relevant body of research for the purposes of this paper stems from the sociological study of social networks and its application to online social networking sites. Social network theory is primarily concerned with the study of actors (nodes) and networks they create (links), as well as the relevance of the depth and strength of social networks. Some of the main ideas within this theory concern sociological questions about relationships, such as connections (e.g. Feld and Carter, 1998; Festinger et al., 1950), homophily (e.g. McPherson, Smith-Lovin &Cook, 2001), distance between nodes (e.g. Freeman & Linton, 1992).

SNT has been applied to ONSs and the issue of privacy by a number of researchers. Most notably, Gross and Acquisti (2005) employ SNT to study information revelation and privacy in online social networks using the example of Facebook. Similarly, following the assumptions of SNT, Houghton and Joinson note a range of phenomena occurring on OSNs, such as convergence of relationships or interconnectivity (2010). While their research largely concerns Facebook, this paper follows similar theoretical frameworks to analyse LinkedIn.

Theoretical Framework

For the purposes of this paper and due to the nature of LinkedIn, the definition of privacy accepted here follows researchers identifying privacy on OSNs as control information about the self revealed to other members of a social network (e.g. Houghton & Joinson, 2010).

As outlined in the introduction, this paper employs two theoretical frameworks to analyse the issues around privacy on LinkedIn, namely social network theory and information revelation. SNT has been applied in the context of OSNs before with particular attention to Facebook and provided a range of valid insights, therefore the application of this theory to LinkedIn follows this thread of research and allows to provide a comparable set of results. Information revelation in the context of OSNs has been studied before in the context of blogging and Facebook; in the study of LinkedIn it seems to be of particular relevance due to the user's capacity to reveal or hide specific information.

The application of SNT to online networks and privacy raises a number of important questions, as outlined in Gross and Acquisti (2005).

- First, online social networks increase polarisation of connections, reducing nuances of a variety of social relationships to binary oppositions: "friend or not" (Boyd, 2004), leading to cases where "people are indicated as Friends even though the user does not particularly know or trust this person" (Boyd, 2004: 80). The same applies to LinkedIn, where the notion of "connection" or "not a connection" does not reflect loose categorisation of weak or strong ties present in the offline world.

- Second, Donath and Boyd claim that "the number of weak ties one can form and maintain may be able to increase substantially [online], because the type of communication that can be done more cheaply and easily with new technology is well suited for these ties" (2004: 80). In fact, LinkedIn seems to encourage entering into a vast number of weak tie connections, and users with many connections seem to be perceived as more valuable within the network.

- Third, OSNs allow the inclusion of hundreds, or on LinkedIn even thousands of direct connections, therefore leading to unprecedented masses of second and third degree connections. This is in sharp contrast with offline social networks, where nodes usually maintain a limited number of significant ties and from 1,000 to 1,700 "acquaintances" or "interactions" (Donath & Boyd, 2004; Strahilevitz, 2004).

Patterns of information revelation on OSNs have been previously studied in the context of Facebook (Gross & Acquisti, 2005). Before analysing this particular case, the authors propose three patterns that they have noticed on different OSNs.

- First, the degree of identifiability of users changes across the types of OSNs. Some OSNs, as the authors note, encourage the use of real names (such as Facebook), while others discourage users from publicly revealing their identities (e.g. dating sites, where often only the first name of a user is revealed in the network).

- Second observation covers the type of information revealed or elicited. The authors noted that these often concern hobbies and interests, through to drinking and drug habits.

- Third, according to the authors visibility of information is highly variable across networks. For example, some networks limit access to personal information to explicitly selected user's network members, while others broadcast information more openly.

Research Setting

LinkedIn is an OSN widely used by professionals across all domains and in many countries (in some, like Germany or Poland, local equivalents are more prominent). The main purpose of the network is to allow professionals to connect with other members for networking within the business context. Members are invited to fill out personal profiles, connect with other members and browse their connections.

The study of 15 member profiles provides the opportunity to analyse in detail how SNT is reflected in practice on LinkedIn and what are the patterns of information revelation among its members. The limited number of members in the sample allows for a detailed enough analysis within a restricted period of time, and yet due to a randomised process of selection the results can be extended to larger member groups.

The sample has been chosen from a group of professional management consultant profiles present on LinkedIn the access to which has been provided through the author's colleague working professionally in the field. The author has set up a separate account for research purposes to be able to clearly identify first, second and third degree connections with the sample profiles. Access to public profiles was obtained through a Google search for respective members and their LinkedIn profiles, while out of network access was obtained through a keyword search based on professional headlines. The analysis was carried out first in terms of the SNT and its three assumptions, and then in terms of the patterns of information revelation.

Results and Analysis

The analysis of 15 member profiles is presented as follows. First, default LinkedIn settings for new member accounts are presented, followed by an analysis of changes of information visibility within single profiles field by field and an analysis of information revealed across all profiles to first, second, third degree connections, public profiles and out of network members.

Default Settings

Default LinkedIn privacy settings reveal all fields depending on the input from member to first degree connections, including "People also viewed" field, all connections and give the possibility to send a message to a user. By default, recommendations are visible to the network (first, second, third degree connections). Members cannot control visibility of information between first, second and third degree connections and by default all fields are visible to the whole network.

Members have a large degree of control over their public profiles and can select which fields are visible in public searches. However, by default, all information is shared and an "Advice for contacting" field is added. Any changes from the default suggest intentional action from a member.

Out of network visibility is, by default, limited to basics, picture and headline, with name and surname hidden (replaced by a placeholder "LinkedIn member"). Members have no control over the visibility to out of network LinkedIn members apart from Open Networker members who by default share all their information even with out of network members.

Degree of Within-Profile Changes

In general, members do not seem to exercise the possibility to change the visibility of information. Only 4 profiles from the sample revealed user intervention in terms of public visibility of information, mostly concerning visibility of pictures. One member exhibited active involvement with the features and decided to hide five fields from his public profile, and another member decided not to reveal seven fields in public.

Revelation by Degree of Connection

First degree connections have access to all information provided by members. Notably, the following fields: "Certifications", "Honors and awards", "Courses", "Projects", "Publications" and "Volunteering" were filled out only in 3, 3, 3, 6, 1 and 1 times out of 15 respectively. It is also worth pointing out again that 5 out of 15 members decided to reveal their date of birth to first degree connections. None of the members in the sample decided to hide his or her connections from first degree connections and only one member decided to hide "People also viewed" box.

Second degree connections have largely a similar extent of access to information. Just in one case, the picture was hidden from second degree connections. Dates of birth of 5 members who decided to reveal them were partially blanked by LinkedIn (leaving just the day and month visible) for second degree connections. 9 out of 15 members decided to reveal recommendations to the whole network, rather than just to direct connections. "Connections" visibility was limited to shared connections only. Second degree connections can only message members through a paid-for InMail function.

Third degree connections, since they are covered under the same "network" as second degree connections have the same visibility over member information. The only exception here is the visibility of "Connections" which are hidden, therefore it is not possible to discover who is the second degree connection between the third degree connection and a member. A third degree connection can ask for an introduction, which is a paid function over a certain limit. Third degree connections can send messages to members only via the paid InMail function.

Public profile visibility is subject to member choice, yet by default every field is visible to everyone and members rarely change these settings (apart from cases described in the within-profile variations section). The only exception is the visibility of pictures (settings for picture visibility are available right below the picture upload box). LinkedIn automatically blocked the visibility of birthday dates and marital statuses of 5 members who revealed it. The same applies to recommendations and connections. It is not possible to message members through public profiles, which explains why 10 members provided information in "Advice for contacting". LinkedIn encourages public profile visitors to set up LinkedIn accounts to be able to contact members.

Surprisingly, out of network profiles have strictly limited visibility, apart from Open Networker profiles. Out of network profiles do not display the name and surname, 3 out of 15 members decided to hide their pictures. LinkedIn encourages out of network visitors to purchase premium accounts to obtain access to member information.

The "Name and surname" field is visible by default to all degrees of connection and in public searches, it is however hidden for out of network members. None of members in the sample selected the possibility to reveal name and initial only to non-first-degree connections. Each profile at each level provides "basics", i.e. approximate location, current employment, education. "Picture" visibility changes and in the sample of 15 profiles, 4 members decided to hide it from public profiles and 3 members decided not to reveal it for out of network members. Fields such as "Current positions", "Past positions", "Education", "Languages" or "Skills", if filled out, were usually shared with the network without any changes.

Findings

Referring back to the theoretical framework of SNT and IR discussed in the previous parts of this paper, analysing the results in comparison to the assumptions of these frameworks is useful to provide a structured overview of privacy issues on LinkedIn.

First, SNT suggests that OSN increase polarisation of connections and reduce them to binary oppositions. As the results indicate, LinkedIn offers a slightly higher portfolio of options, from first, second and third degree connections through to public profiles and out of network. However, members have control only over their first degree connections that can be manually added or removed from the network, not over other degrees. Moreover, LinkedIn does not provide facilities to control which information is visible to which degrees of connections between first, second and third degrees (collectively "the network"). Unlike in offline networks, LinkedIn does not have the capacity to manage nuanced relationships or reveal only certain pieces of information to certain groups (or even individual) of members.

Second, it has been suggested that the use of OSN can substantially increase the number of weak ties. The results confirm that though it is impossible to measure the increase of the number of weak ties online as opposed to offline, LinkedIn employs a variety of measures encouraging connecting with members who are relatively poorly known or even unknown. LinkedIn, for example, allows members to connect through membership in the same group on LinkedIn. The Open Networker function on LinkedIn encourages members to connect with other members they do not know but who indicated they are willing to connect with any other user.

Third, by allowing the inclusion of hundreds or thousands of first degree connections, OSNs lead to unprecedented amounts of second and third degree connections within one's network. This seems to have been confirmed through the study conducted. The LinkedIn account used for its purposes at one point in time had just 1 first degree connection and LinkedIn signalled that it gave access to 380,162+ members as second and third degree connections. An average user from the sample tested had 427 connections giving access to 5,576,901+ second and third degree connections. The author's own LinkedIn account has 2,539 connections giving access to 13,731,237+ members within the network. This is the number of people whose information visibility is revealed and who can be contacted or introduced to.

In terms of patterns of information revelation, the degree of identifiability on LinkedIn is high. The network, for the purposes it has been created, encourages members to use real names and surnames to increase their trustworthiness, searchability and findability. Members have the option to hide their full surname for third degree connections, yet research revealed that very few do that. Moreover, 5 members in the sample shared their dates of birth with first degree connections which were only partially hidden automatically by LinkedIn.

The type of information revealed on LinkedIn is strictly professional and fits the purpose of the network. The only free text area allowing uncontrolled input is the "Summary" section, and following van Dijck's (2013) suggestions, members tend to use narratives rather than resume-like facts. However, it is interesting to consider the prescriptive role of LinkedIn's interface in this respect; perhaps by inviting members to provide other information ("Tell us something about yourself" or "What do you do in your spare time") the network would increase the amount of non-professional information shared.

Visibility of information is high within the network, including first, second and third degree connections. LinkedIn automatically blocks potentially risky information, such as dates of birth, from being visible to second and third degree connections. Members themselves tend to opt for high information visibility and do not actively manage their public profiles. This, however, is due to the purpose of the network. It is also interesting that there are different levels of visibility for paid LinkedIn members, namely premium and recruiter accounts.

It is worth noting that the author has indeed purchased a premium account to investigate visibility of out of network profile information. However, upon purchasing, it was revealed that access to full profile information out of network is available to recruiter accounts only.

After a further investigation it was revealed that recruiter accounts indeed have access to all out of network profiles and are able to contact out of network members through InMail. LinkedIn advertises this option suggesting "expand your searches beyond your personal connections to access the entire LinkedIn network" (LinkedIn, 2014). Full out of network visibility is available with Recruiter Corporate account (currently priced at 499.95 GBP pcm).

In 2013, this service was used by over 16,000 companies all over the world and the LinkedIn Recruiter platform became the flagship product of the company. According to one article:

> Recruiter already offers several unique features that are incredibly hard for companies to build or find elsewhere: a giant data set of more than 200 million users and growing, a way to engage passive employees, and the ability to build career branding around a company. The value of the LinkedIn's data is clear — it would take companies years and years to build a candidate pool even a fraction of that size, and it would be nearly impossible to keep up to date (Chang, 2013).

In the light of the above, it would be interesting to research how perceptions of privacy of information change when members are made aware that the network they use is, in fact, selling access to their information (initially not necessarily private or raising concerns) and members have no knowledge or control over who is viewing their full profiles (recruiters

can make themselves anonymous on "People who viewed your profile"). Even from the outset, this may suggest a breach of the trust that members have in the network and act against SNT, allowing recruiters who pay to make shortcuts in social networks.

Conclusions

As supported by the research conducted, social network theory and the patterns of information revelation present on LinkedIn expose members to a number of privacy risks.

First, increased polarisation of connections can lead to the infiltration of a member's network because even though some pieces of information should be available to first connections only, it seems to be easy to connect on LinkedIn under false pretence to obtain access to restricted information, such as date of birth.

Second, a sharp increase of the number of weak ties may lead to the risk of secondary data collection, i.e. collecting information on members' use of the network, such as length of connections, other profiles visited or messages sent (Hogben, 2007).

Third, due to a high degree of identifiability (for example photos are always identifiable and 100% of members from the tested sample used their real names), there is a high risk of re-identifiability, profile squatting on other networks or services or reputation slander.

Fourth, the type of information revealed on LinkedIn, i.e. aiming at providing as full an account of one's professional life as possible, may lead to a digital dossier aggregation, with profiles downloadable by third parties.

Fifth, high visibility of information may result in stalking and bullying, where cyberstalking can be identified as threatening behaviour in which a perpetrator contacts a victim by electronic means, such as email, instant messaging, or in the case of LinkedIn – InMail (Hogben, 2007).

Many authors agree, and the findings in this paper support the thesis, that OSNs by default set many pieces of information as publicly available, while members do not understand privacy settings available to them. Moreover, as has turned out to be the case on LinkedIn, members do not fully understand what they reveal and to whom.

The analysis conducted in this paper furthers the understanding of information revelation patterns on online social networks and points to the extent in which members act upon the possibility to tailor the amount of information revealed. The paper also applies social network theory to a new platform, providing insights into its functioning, but also further validating and confirming previous results of similar studies.

This paper covered just the aspects of privacy in terms of information shared with other members, but as mentioned in the introduction, privacy risks may concern breaches by service providers themselves as well as third-party applications. Therefore it would be interesting to research these areas in relation to LinkedIn further.

References

Altman, I. (1975) *The Environment and Social Behavior*. Belmont, CA: Wadsworth.

Anderson, J., Stajano, F. (2013) Must Social Networking Conflict with Privacy? *IEEE Security & Privacy*, May/June 2013: 51–60.

Art Institute (2011) *Online Social Media: An Open Door to Your Privacy?* Available at http://insite.artinstitutes.edu/online-social-media-an-open- door-to-your-privacy-20838.aspx, accessed 3rd April 2014.

Ayalon, O., Toch, E. (2013) Retrospective Privacy: Managing Longitudinal Privacy in Online Social Networks. *Symposium on Usable Privacy and Security (SOUPS) 2013*, July 24–26, 2013, Newcastle, UK.

BBC (2014) *LinkedIn Email Addresses Exposed by Plug-In Software*, available at http://www.bbc.co.uk/news/technology-26833863, accessed on 26th March 2014.

Boyd, D. (2004) Friendster and Publicly Articulated Social Networking. *In Conference on Human Factors and Computing Systems (CHI 2004)*, April 24-29, Vienna, Austria, 2004.

Boyd, D., Ellison, N. (2007) Social Network Sites: Definition, History, and Scholarship. *J. Comp.-Mediated Commun*., 13(1): 210-230.

Burgoon, J. K., Parrott, R., le Poire, B. A., & Kelley, D. L. (1989) Maintaining and Restoring Privacy through Communication in Different Types of Relationships. *Journal of Social and Personal Relationships*, 6(2): 131–158.

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* 29: 437–448.

Cavoukian, A. (2011) *LinkedIn Founder Dead Wrong about Privacy Being Just for 'Old People'*, available at: http://www.itbusiness.ca/blog/linkedin-founder-dead-wrong-about-privacy-being-just-for-old-people/20503, accessed on 26th March 2014.

Cendella, M. (2011) *Privacy is for Old People Says LinkedIn Founder*. Available at: http://www.theladders.com/career-newsletters/privacy-is-for-old-people-says-linkedin-founder, accessed on 26th March 2014.

Chang, A. (2013) The Most Important LinkedIn Page You've Never Seen. *Wired*, available at: http://www.wired.com/2013/04/the-real-reason-you-should-care-about-linkedin/, accessed on 28th March 2014.

Change.org (2013) *LinkedIn: Protect your Users from Stalkers and Help Keep Victims Safe.* Available at: https://www.change.org/petitions/linkedin-protect-your-users-from-stalkers-and-help-keep-victims-safe. Accessed on: 26 March 2014.

DeCew, J. W. (1997) *In Pursuit of Privacy: Law, Ethics, and the Rise of Technology*. Ithaca, NY: Cornell University Press.

Donath, J., Boyd, d (2004) Public Displays of Connection. *BT Technology Journal*, 22: 71–82.

Feld, S. L., & Carter, W. C. (1998) Foci of Activity as Changing Contexts for Friendship. In R. G. Adams & G. Allan (Eds.), *Placing Friendship in Context*, Cambridge, UK: Cambridge University Press.

Festinger, L., Schachter, S., and Back, K. (1950) *Social Pressures in Informal Groups*. New York: Harper and Bros.

Floridi, L. (2011) The Construction of Personal Identities Online. *Minds & Machines* (2011) 21:477–479.

Freeman, Linton C. (1992) The Sociological Concept of "Group": An Empirical Test of Two Models. *American Journal of Sociology* 98(1): 152-166.

Gao, H. et al. (2011). *Security Issues in Online Social Networks*. IEEE Internet Computing, IEEE Computer Society, 56 -63.

Goffman E (1959) *The Presentation of Self in Everyday Life*. New York: Anchor Books.

Granovetter, Mark S. 1973. The Strength of Weak Ties. *American Journal of Sociology* 78, 1360-1380.

Gross, R. and Acquisti, A. (2005) Information Revelation and Privacy in Online Social Networks. *WPES'05* (71- 80). Alexandria, VA: ACM.

Haefner R. (2009) More Employers Screening Candidates via Social Networking Sites, available at: http://www.careerbuilder.com/Article/CB-1337-Getting-Hired-More-Employers-Screening-Candidates-via-Social-Networking-Sites/, accessed on 1st April 2014.

Hogben, G., ed. (2007) Security Issues and Recommendations for Online Social Networks. *ENISA Position Paper No.1*.

Hongladarom, S. (2011) Personal Identity and the Self in the Online and Offline World. *Minds & Machines* 21: 533–548.

Houghton, D., Joinson, A. (2010) Privacy, Social Network Sites, and Social Relations. *Journal of Technology in Human Services*, 28: 74–94.

Lacter, M. (2009) Reid Hoffman LinkedIn. *Inc.*, *31*(4), 82-84.

Madia, S. (2011) Best practices for using social media as a recruitment strategy. *Strategic HR Review,* 10(6): 19-24.

Marshall, N.J. (1972) Privacy and Environment. *Human Ecology* 1972, 1(2): 93-110.

Marshall, N.J. (1974) Dimensions of Privacy Preferences. *Multivariate Behavioral Research* 1974, 9(3): 255-271.

McPherson, M., Smith-Lovin, L., and Cook, J. (2001) Birds of a Feather: Homophily in Social Networks. *Annual Review of Sociology* 274: 15-44.

Peachey, K. (2012) The New Boys Club: The Effect of Gender on LinkedIn Profiles. *2012 Student Paper Competition*, Elizabethown College.

Pedersen, D.M. (1979) Dimensions of privacy. *Perceptual and Motor Skills* 1979, 48(3): 1291-1297.

Qi, M., Edgar-Nevill, D. (2011) Social Networking Searching and Privacy Issues. *Information Security Technical Report,* 16: 74-78.

Rodogno, R. (2011) Personal Identity Online. *Philos. Technol.* (2012) 25:309–328.

Sherman, E. (2013) *LinkedIn Intro: Security, Privacy--You Name It, There's a Problem*, available at: http://www.inc.com/erik-sherman/linkedin-intro-security-privacy-you-name-it-theres-a-problem.html, accessed on 26th March 2014.

Solove, D. J. (2007) *The Future of Reputation: Gossip, Rumor, and Privacy on the Internet.* New Haven: Yale University Press.

Strahilevitz, L. (2004) A Social Networks Theory of Privacy. The Law School, University of Chicago, *John M. Olin Law & Economics Working Paper No. 230* (2D Series).

Tomlinson, A., Yau, P., MacDonald, J. (2010) Privacy Threats in a Mobile Enterprise Social Network. *Information Security Technical Report*, 15: 57 -66.

Van Dijck, J. (2013) 'You have one identity': performing the self on Facebook and LinkedIn. *Media Culture Society* 2013 35: 199 – 215.

Van Eecke, P., Truyens, M. (2010) Privacy and Social Networks. *Computer Law & Security Review 26*, 535 – 546.

Veldt, D. (2013) *LinkedIn: The Creepiest Social Network*. Available at: http://www.interactually.com/linkedin-creepiest-social-network/. Accessed on: 26 March 2014.

Warren, S. V., & Brandeis, L. D. (1890) The Right to Privacy. *Harvard Law Review*, 4(5): 193-220.

Watts, D., Dodds, P, Newman, M. (2002) Identity and Search in Social Networks. *Science, New Series*, Vo. 296, No. 5571, 1302 – 1305.

Westin, A. F. (1967) *Privacy and Freedom*. New York: Athenaeum.

Whitley, E., Gal, U., Kjaergaard, A. (2014) Who Do You Think You Are? A Review of the Complex Interplay between Information Systems, Identification and Identity. *European Journal of Information Systems* (2014) 23, 17–35.

YouTube (2010). *Davos Annual Meeting 2010 - The Growing Influence of Social Networks*, available at: https://www.youtube.com/watch?v=pexGCUPlUeA&feature=player_detailpage#t=13m, accessed 26th March 2014.

YouTube (2011). *Visualize your LinkedIn network with InMaps*, available at: https://www.youtube.com/watch?v=PC99Nw2JX8w, accessed 1st April 2014.

YouTube (2013). *LinkedIn Privacy Policy*, available at: https://www.youtube.com/watch?v=xIW5RI8K3Yg, accessed 1st April 2014.

Zhang, C., Sun, J. et al (2010). Privacy and Security for Online Social Networks: Challenges and Opportunities. *IEEE Network*, July/August, 13-18.