SI: Re-Imagining a More Trustworthy Social Media Future

SM+S
social media + society

Cybervetting and the Public Life of Social Media Data

Social Media + Society
April-June 2020: 1–13

DOI: 10.1177/2056305120915618
journals.sagepub.com/home/sms
SAGE

Anatoliy Gruzd[1], Jenna Jacobson[1], and Elizabeth Dubois[2]

Abstract

The article examines whether and how the ever-evolving practice of using social media to screen job applicants may undermine people's trust in the organizations that are engaging in this practice. Using a survey of 429 participants, we assess whether their comfort level with cybervetting can be explained by the factors outlined by Petronio's communication privacy management theory: culture, gender, motivation, and risk-benefit ratio. We find that respondents from India are significantly more comfortable with social media screening than those living in the United States. We did not find any gender-based differences in individuals' comfort with social media screening, which suggests that there may be some consistent set of norms, expectations, or "privacy rules" that apply in the context of employment seeking—irrespective of gender. As a theoretical contribution, we apply the communication privacy management theory to analyze information that is *publicly* available, which offers a unique extension of the theory that focuses on private information. Importantly, the research suggests that privacy boundaries are not only important when it comes to private information, but also with information that is publicly available on social media. The research identifies that just because social media data are public, does not mean people do not have context-specific and data-specific expectations of privacy.

Keywords

social media, privacy, job screening, social media screening, cybervetting, communication privacy management

Introduction

In recent years, there has been a growing concern of how social media platforms are being used by so-called "bad actors" for misinformation and disinformation campaigns and how these platforms may be creating echo chambers and silos in our society. Another trend of critical importance that has received little attention in academic research is how third parties (mis)use the public's social media data—especially when such data are publicly available and do not require users' consent to be mined. This practice is problematic because even if social media posts are public, people may still have context-specific expectations of privacy (Dubois et al., 2020; Jacobson et al., 2020; Jacobson & Gruzd, 2020; Nissenbaum, 2018; Quinn & Papacharissi, 2018), which gives rise to "fuzzy boundaries" of privacy management (Child & Starcher, 2016).

The issue of trust is particularly pronounced when considering the increased use of publicly available social media data by organizations for *cybervetting*. Cybervetting, also known as social media screening, refers to the use of social media to attract, recruit, and screen qualified job applicants. According to a recent survey of hiring managers, the number of organizations in the United States that use social media to screen job applicants has increased from 11% in 2006 to 70% in 2018 (CareerBuilder, 2018). When researching job applicants on social media, organizations seek to validate candidates' qualifications, assess whether candidates present themselves professionally, and ensure that candidates are not posting any abusive or harassing content (CareerBuilder, 2018). Cybervetting is perceived as providing an opportunity for employers to obtain "trustworthy information" (Berkelaar, 2014). Not only is the availability of social media data attractive to organizations, there is also early evidence to suggest that these data can be a proxy to assess job candidates' personality traits (Stoughton et al., 2013), as well as to predict

[1]Ryerson University, Canada
[2]University of Ottawa, Canada

Corresponding Author:
Anatoliy Gruzd, Ted Rogers School of Management, Ryerson University, 350 Victoria Street, Toronto, Ontario M5B 2K3, Canada.
Email: gruzd@ryerson.ca

key metrics, including academic ability and job performance (Kluemper et al., 2012).

As downsizing spread in the 1980s, employees engaged in a positive self-presentation activity and reframed their value explicitly in their resumes; consequently, employers began to distrust the information that prospective employees shared (Barrick et al., 2009; Berkelaar, 2014). Hedenus et al. (2019) found that cybervetting helps employers determine whether the candidate is trustworthy. For example, employers assess a job candidate's online connections to see if there are any mutual connections to assess trustworthiness (Berkelaar & Buzzanell, 2015). Although cybervetting is useful for hiring organizations, this practice is often not disclosed to job applicants, which could lead to diminished trust.

We surveyed 429 participants to analyze their comfort with cybervetting from job seekers' perspectives. While much of the organizational and communication research has approached social media screening from the perspective of employers, there are some exceptions; for example, Root and McKay (2014) analyzed job seekers' awareness of this hiring practice and found that as many as 80% of respondents believed that employers are checking job applicants' social media activities, which points to widespread awareness of social media screening. We expand this line of research beyond investigating whether people are aware of this hiring practice by measuring how comfortable job applicants are with this practice and what factors contribute to their attitudes. Specifically, we examine five factors shown to guide people's privacy rules, as proposed by the communication privacy management (CPM) theory: culture, gender, motivation, risk-benefit ratio, and context (Petronio, 2002). We find that individuals have context and data-specific privacy boundaries even when the information is publicly available. At a practical level, the research provides a granular understanding of job seekers' attitudes about social media screening by delineating different factors influencing their perception. The findings assist organizations and hiring managers to develop best practices that are aligned with job applicants' expectations. At a theoretical level, we apply the CPM theory and evaluate its applicability when using publicly available information, rather the private information.

Literature Review

Social Media Screening Practices

There are unique opportunities and challenges for organizations seeking to leverage social media for hiring, yet "social media data are vast, noisy, distributed, unstructured, and dynamic" (Gundecha & Liu, 2012, p. 4). Previous research in this area has primarily focused on whether and how organizations and recruiters use social media for hiring purposes—or so-called "cybervetting"—which has become the norm, rather than the exception (Berkelaar & Buzzanell, 2015; Ghoshray, 2013; Jeske & Shultz, 2019). In a small-scale study with a focus on LinkedIn use, Zide et al. (2014) found that recruiters usually used the site to look for applicants' "employment history, education, years of experience, and how the applicant presents him or herself on the site" (p. 589). A total of 60% of the participants indicated that they consider how well-connected the applicants are in the hiring process. Ollington et al. (2013) identified the following four distinct mechanisms recruiters use on various social networking sites: (1) connecting job seekers through secondary connections and establishing themselves as highly connected nodes in online social networks, (2) building their own online brand, (3) offering job seekers access to specialized online resources that are normally only available to recruiters, and finally, (4) acquiring accurate data about job seekers. And while employers' use of social media can positively influence corporate reputation and indirectly increase job applicants' intention to apply for a job with an organization (Sivertzen et al., 2013), there are some potential risks and challenges associated with using social media for attracting, recruiting, and screening job applicants, including negative biases toward minorities (Ruggs et al., 2016), legal concerns (Schmidt & O'Connor, 2016), misrepresentation, and misattribution of job applicants (Frantz et al., 2016).

Studies of Prospective Employees

Previous research that examines job applicants' perspectives is limited, but often explores job seekers' self-disclosure practices on social media by examining factors that influence what job seekers share, delete, or decide not to share on social media. Research in this area is often focused on inappropriate self-disclosure on social media, which include posting informal selfies or tagged photos, commenting on controversial topics, or "participation in activities which are in violation of university or workplace policy" (Peluchette & Karl, 2008, p. 418). El Ouirdi et al. (2015) examined the relationship between self-disclosure and the following factors: (1) the motivation to maintain a professional online image, (2) social media self-efficacy, and (3) the perceived effectiveness of social media in the job search context. One particularly interesting finding was that social media self-efficacy was found to be positively associated with job seekers' self-disclosure of both inappropriate and career-oriented content, which the authors attributed to the increased use of social media and loss of inhibition. Zide et al. (2014) studied the relationship between the information LinkedIn users share and their occupation for three occupation groups: HR, sales/marketing, and industrial-organizational psychologists (I-O psychologists). Unsurprisingly, the authors found that sales/marketing professionals were the most "networking-savvy" of the three groups, and therefore, have an advantage. Similarly, Wu (2013) evidenced that social media can be used to positively impact an employee's network position.

Another line of research examines prospective employees' awareness of social media screening practices by organizations and recruiters. Root and McKay (2014) found that students are becoming increasingly aware of this practice—80% of respondents felt that prospective employers were likely to check their social media profiles. The authors found that students were generally comfortable with the practice as they tended to *disagree* with the statement: "it is wrong for anyone to consider what they have posted on the internet when applying for a job." Stoughton et al. (2015) came to a somewhat different conclusion in their research: the practice of screening applicants on social media increased students' sense of an invasion of privacy—regardless of whether a student was offered a job in their experimental study or not. In another study, Berkelaar (2014) found that applicants would like organizations to be transparent about cybervetting, and participants also expressed a feeling of resignation about this practice. Accordingly, there are inconsistent findings as to the public's perception and comfort with the practice of social media screening.

To investigate possible reasons behind these somewhat divergent findings, our research extends the previous literature in several ways. Similar to Root and McKay (2014), we examine the relationship between different types of social media data and the practice of screening job applicants using social media. But instead of asking what information prospective employees think is *important* to employers, we ask participants what information would be *acceptable* for potential employers to access. We also go beyond studying readily-accessible data and metadata to include more complex data types that can and are used by companies, such as sentiment and social network-related information. Related work (Osatuyi, 2015; Wang et al., 2011) examined social media users' privacy attitudes, but without providing any particular context in terms of who is accessing users' social media data and for what purposes. We address this limitation by focusing on the use of social media data by organizations in the context of screening job applicants—as privacy needs to be considered in a context (Nissenbaum, 2009). Finally, as most previous studies surveyed job seekers or students, we use a more diverse population of social media, including job seekers and non-job seekers.

Theoretical Framework

The CPM theory introduced by Petronio (2002) explores how people regulate information they consider to be private, which provides a framework to reconcile the tension between revealing and concealing information. The theory contends that privacy management is dialectic in that people need to disclose private information in order to fulfill social functions and needs, while also concealing information in order to maintain their privacy. The dialectic refers to the push and pull that people experience when deciding to conceal or disclose information as privacy boundaries are negotiated (Baruh et al., 2017). People make purposeful decisions based on the desire to disclose and the desire to protect their personal privacy; the disclosure choices are as important as non-disclosure decisions (Serewicz & Petronio, 2007).

CPM is built on Altman and Taylor's (1973) social penetration theory, which argues that people use self-disclosure as a way to build relationships, but also recognizes that there are both costs and rewards to disclosure. Building on this theory, Petronio (2002) notes that individuals desire privacy, yet also want to self-disclose to build relationships. While the theory grew out of interpersonal and family research, it has also been successfully applied to the disclosure of private information in other contexts, including online information privacy. For example, Waters and Ackerman (2011) relied on CPM to ask what are the benefits and consequences of disclosure, and is there a difference in online disclosure between men and women. Others use CPM to explore topics such as people's private disclosures in the workplace (Smith & Brunner, 2017), privacy management of bloggers (Child et al., 2012), boundary turbulence on Facebook (DeGroot & Vik, 2017), privacy controls on Facebook (Cavusoglu et al., 2016), and college students' voluntary disclosure on Facebook (Waters & Ackerman, 2011).

CPM outlines that people develop privacy rules, which, in the context of our research, can be defined as strategies that individuals use to decide what, when, and where to post on social media. According to CPM, the privacy rules are based on the following five factors (Child et al., 2012; Petronio, 2002): (1) Culture: every culture has a particular set of privacy values; (2) Gender: gender differences contribute to people's privacy rules; (3) Motivations: motivations and needs influence when people tend to be more open or private; (4) Risk-benefit ratio: people calculate the risks and benefits of disclosing information; and (5) Context: people feel the need to disclose information based on the specific situation. In our study, we ground the five factors as follows:

Culture. We compare survey data between people from two different cultures: India (113 people) and the United States (319 people). It is well researched and widely understood that the United States is a highly individualistic society, versus India which is a collectivist society (Kumaraguru et al., 2005). As the privacy literature shows that cultural and regulatory differences (Bellman et al., 2004) influence information privacy concerns, we ask,

> RQ1: Do people living in India react to cybervetting differently than those in the United States?

Because privacy attitudes of knowledge workers (Patil et al., 2010) and social media users (Wang et al., 2011) in India tend to be lower than those in the United States, we hypothesize,

> Hypothesis 1: Social media users in India are more comfortable with cybervetting than users in the United States.

In the context of our research, we use *cybervetting* to refer to the practice of screening job applicants on social media, specifically using publicly available data.

Gender. We compare the comfort levels of social media screening between men and women.[1] Previous work suggests that women have a higher level of privacy concerns in comparison to men in the context of internet and social media use (Bartel Sheehan, 1999; Cho & Hung, 2011; Youn & Hall, 2008). Thus, we ask,

> RQ2: Do women react to cybervetting differently than men?

In the context of internet and social media use, previous work suggested that women tend to have a higher level of privacy concerns than men (Bartel Sheehan, 1999; Cho & Hung, 2011; Youn & Hall, 2008). Thus, our second hypothesis is the following:

> Hypothesis 2: Women are less comfortable with cybervetting than men.

Motivations. We compare the comfort levels of job seekers and non-job seekers as they have different motivations and needs for sharing information on social media. As most literature has either focused on people who are actively seeking employment or students who presumably will soon seek employment, we contribute to this research area by comparing attitudes between likely job seekers and those who are not seeking employment. Thus, we ask,

> RQ3: Do job seekers react to cybervetting differently than non-job seekers?

We expect that job applicants may be engaged in selective self-presentation to present themselves in a professional manner and improve their online image (Batenburg & Bartels, 2017; Roulin, 2014). Therefore, our next hypothesis is,

> Hypothesis 3: Job seekers are more comfortable with cybervetting than non-job seekers.

Risk-Benefit Ratio. To provide nuance to understand how people assess the risk-benefit ratio, we ask participants a series of questions to measure their general privacy concerns related to the handling of their social media data. Under this factor, we examine whether there is an association between users' privacy concerns (more broadly) and their comfort level with a specific practice (organizations' use of publicly available social media data to screen job applicants). We ask,

> RQ4: Is there a relationship between users' privacy concerns on social media and their attitude toward cybervetting?

Following early work on cybervetting that showed that job applicants' privacy concerns negatively impact their overall fairness perception of the search process as well as their attraction toward the hiring organization (Bauer et al., 2006; Madera, 2012; Stoughton et al., 2015), we propose the following hypothesis:

> Hypothesis 4: Social media users who have higher privacy concerns are less comfortable with cybervetting.

In accordance with CPM, people will assess both the risks and benefits associated with this particular use of social media data. Thus, if we discover that users' higher privacy concerns are associated with a lower comfort level with the above-mentioned practice, then this may suggest that privacy risks outweigh perceived benefits. But if benefits outweigh risks, we may discover that there is no relationship between general privacy concerns and the comfort level with the practice (so-called "privacy paradox").

Context. Context matters as people's beliefs, concerns, and practices are contextually situated (Nissenbaum, 2009, 2018). As such, it is important that the study is grounded in the specific context of organizations using publicly available social media data to screen job applications. To bolster the internal validity of the research, we maintain one context; as such, there is no research question associated with this factor.

Method

Recruitment through Amazon Mechanical Turk

We collected data using Amazon Mechanical Turk (AMT). AMT is a crowdsourcing service organized like a marketplace where requesters can post an online task, such as a survey, and individuals anywhere in the world (called "turkers") can complete this task for compensation (Mason & Suri, 2012). Research indicates that turkers perform tasks primarily to supplement their income (61%) and for personal enjoyment (41%; Paolacci et al., 2010). AMT's pool of potential participants has been relatively stable over time and includes a sample comparable to standard internet samples (Buhrmester et al., 2011) and other more traditional samples (Goodman et al., 2013). In a study that evaluated the internal and external validity of AMT-based samples, Berinsky et al. (2012) found that AMT samples were more representative of the US population than in-person "convenience" samples, but less representative than internet-based panels or national probability samples. The researchers also concluded that turkers tend to be older (M_{age}=32.3, SE=0.5) than student samples (M_{age}=20.3, SE=8.2), but younger than adult samples (M_{age}=45.5, SE=0.9). AMT has implemented a number of mechanisms to ensure the high-quality pool of respondents; for example, every time a turker completes a given task, a requester has an opportunity to review their work and

either approve or reject it. Thus, each turker is assigned an overall approval rating of their tasks, which, in turn, can be used to exclude turkers whose approval rate is less than a specified threshold. Previous work has also evaluated the quality of data collected through AMT and confirmed comparable quality to collecting data by more traditional means. Rand (2012) found that turkers complete the demographic questions truthfully, and a study by Hauser and Schwarz (2016) revealed that turkers were more attentive to the instructions than a comparable sample of college students.

Prior to beginning our study, Research Ethics approval was obtained from two universities. The survey was open for 3 days between December 22 and 25, 2016. Turkers were paid US$1 per response. The average survey completion time was just under 10 minutes, which represents a compensation rate of US$6/hour and is generally higher than what was reported in other studies using AMT (Berinsky et al., 2012; Wang et al., 2011).[2] To ensure high quality of our data collection, we specified that only turkers with an overall approval rate of 75% or higher were eligible to participate in the survey. We also inserted a "trap question" as an attention check to ensure that participants were carefully reading the questions. In total, we received 506 responses. We further cleaned our dataset by excluding 33 responses that did not answer the trap question correctly, 18 responses that were completed in less than 3 min, and one response where the participant did not have any social media accounts (an outlier). In total, the dataset comprised 454 responses.

Considering that our sample primarily consisted of people from the United States and India, we excluded participants from other countries so that we could focus on comparing populations from two different countries. We also excluded three participants who elected not to specify their gender. At the end of the sample selection procedure, 429 responses remained in the final dataset that was used for analysis.

Survey Design and Measurement Model

The survey consisted of three sections. Section 1 asked 17 questions to measure users' Concern for Social Media Information Privacy (CFSMIP) by Osatuyi (2015), which built on a widely accepted construct of Concern for Information Privacy (CFIP) by Stewart and Segars (2002). CFSMIP measures an individual's concerns for information privacy in response to an organization's use or potential use of their personal information across the following four dimensions: collection (COL), errors (ERR), secondary use (SUS), and unauthorized access (UAC). Even though there are a number of alternative approaches to measure privacy concerns on social media (e.g., Dinev et al., 2013; Krasnova et al., 2009; Malhotra et al., 2004), we chose to use CFIP, and specifically its social media version—CFSMIP—because of its emphasis on the organizational use of data which fits well with the focus of this research on employers' use (as opposed to personal use) of social media data (Gruzd & Hernández-García, 2018). The CFSMIP-related questions were general in nature and were not limited to the hiring context (see Table 1).

Section 1 also included the trap question, "Please select 'strongly agree' as your answer choice." Before proceeding to Section 2, all participants read a textual brief about the practice of using social media data to screen prospective employees and some common ways organizations may use such information. In Section 2, participants scored their comfort level (on a scale of 1–7; 1-"very uncomfortable" to 7-"very comfortable") with a potential employer viewing their publicly accessible information from social media. This question was repeated nine times, each with one of the nine sample information types, selected from the following three broad categories: (1) *Raw Data & Metadata*: readily available information, (2) *Analytics*: information that requires some processing, and (3) *Social Networks*: information related to users' online social network (see Table 2). The information type questions were presented in random order to avoid bias. To account for further potential biases in how participants perceive different representations of information types, we randomly assigned them to one of two groups: Group A saw a visual representation of the information type and Group B saw a textual description of the same information type.

The survey instrument was developed and evaluated over a 1-year period to ensure that all text and visual elements were clearly visible and able to be properly interpreted by participants. For example, we used neutral colors whenever possible to avoid a potential color bias in visualizations. Furthermore, we displayed two versions of each visualization depicting different possible outcomes to emphasize that the shown visualizations were only for demonstration purposes. For example, when showing a hypothetical result of sentiment analysis (see Figure 1), one visualization showed the majority of posts were positive (displayed on the left), while the other visualization showed the majority of posts were neutral and a significant proportion of negative posts (displayed on the right).

In the final section of the survey, participants were asked about their overall social media use (i.e., what platforms they used and their frequency of use), as well as general demographic data (i.e., age, country, and education level). We also asked questions about participants' awareness of cases of social media misuse and whether they have been a victim of a data privacy violation.

Statistical Tests

To analyze the data, we used the Automatic Linear Modeling (LINEAR) implemented in the software package SPSS, version 24 (Yang, 2013). The model building method was "Best Subsets" using the Adjusted R Square criterion to select the best performing model. Unlike the stepwise method, the best subset method considers all possible regression models based on available predictors (Oshima & Dell-Ross, 2016); thus, avoiding a potential bias by not deciding on the order of

Table 1. Social Media Information Privacy Construct—CFSMIP (adopted from Osatuyi, 2015; Stewart & Segars, 2002).

To what extent do you agree with the following statements (7-point agreement/disagreement scale)	
Collection (COL)	
COL1	It usually bothers me when social media sites ask me for personal information
COL2	It usually bothers me when social media sites ask me for my current location information
COL3	It bothers me to give personal information to so many people on social media
COL4	I am concerned that social media sites are collecting too much personal information about me
Errors (ERR)	
ERR1	Social media sites should take more steps to make sure that personal information in their database is accurate
ERR2	Social media sites should have better procedures to correct errors in personal information
ERR3	Social media sites should devote more time and effort to verifying the accuracy of the personal information in their databases before using it for recommendations
Secondary use (SUS)	
SUS1	Social media sites should not use personal information for any purpose unless it has been authorized by the individuals who provide the information
SUS2	When people give personal information to social media sites for some reason, these sites should never use the information for any other purpose
SUS3	Social media sites should never share personal information with third-party entities unless authorized by the individual who provided the information
Unauthorized access (UAC)	
UAC1	Databases that contain personal information should be protected from unauthorized access no matter how much it costs
UAC2	Social media sites should take more steps to make sure that unauthorized people cannot access personal information on their site
UAC3	Databases that contain personal information should be highly secured
UAC4	Social media sites should delete a user's account if they illegally access another user's personal information

Table 2. Categories of Information Types.

Raw data & metadata	Analytics	Social networks
Posts: User's text-based posts	Frequent words: Words used frequently by the user	Top posters: Top 10 users who posted in a group
Photos: User's photographs	Post frequency: User's posting frequency	Followers: User's followers/friends
Geolocation: Locations where the user posted from (city and street level)	Sentiment: Sentiment analysis of posts (positive, negative, or neutral)	Communication network: Who is connected to whom in a group

variable entry into the model (Huberty, 1989). One of the advantages of using LINEAR is that it automatically trims outliers by setting them to a cut-off value of three standard deviations from the mean. Furthermore, LINEAR has been shown to be more robust against Type I and II errors relative to more traditional linear regression modeling (Yang, 2013).

For the purposes of the study, the following variables were used as independent variables: *Country*: India (1) or the United States (0); *Gender*: female (1) or male (0); *Job seeking status*: ranging from 1-"very unlikely" to 7-"very likely" ("How likely are you to seek employment within the next 6 months?"); *COL*: privacy concerns related to data collection by social media sites; *SUS-UAC*: privacy concerns related to the secondary use and unauthorized access of social media data; and *ERR*: privacy concerns related to social media sites and organizations storing inaccurate information about users. Each privacy-related factor was calculated as the mean of its corresponding 7-point Likert-type scale questions.

Even though *SUS* and *UAC* were originally envisioned as two separate constructs (Stewart & Segars, 2002), in the social media context, using an exploratory factor analysis, we discovered that SUS and UAC load on a single dimension, which is similar to what Osatuyi (2015) found in their dataset as well.

The dependent variable (*HRComf*) was calculated as the mean of the comfort level questions (7-point Likert-type scale) asked in relation to the seven different information types: Posts, Photos, Geolocation, Sentiment, Top Posters, Followers, and Communication Network. To eliminate a potential bias, two information types (Frequent Words and Post Frequency) were excluded from the composite comfort score as there was a difference in how participants evaluated these two information types depending on whether the questions were displayed with or without the accompanying visual representations (see Gruzd et al., 2017a, 2017b). Since there were no groupings in responses among different information types, we concluded

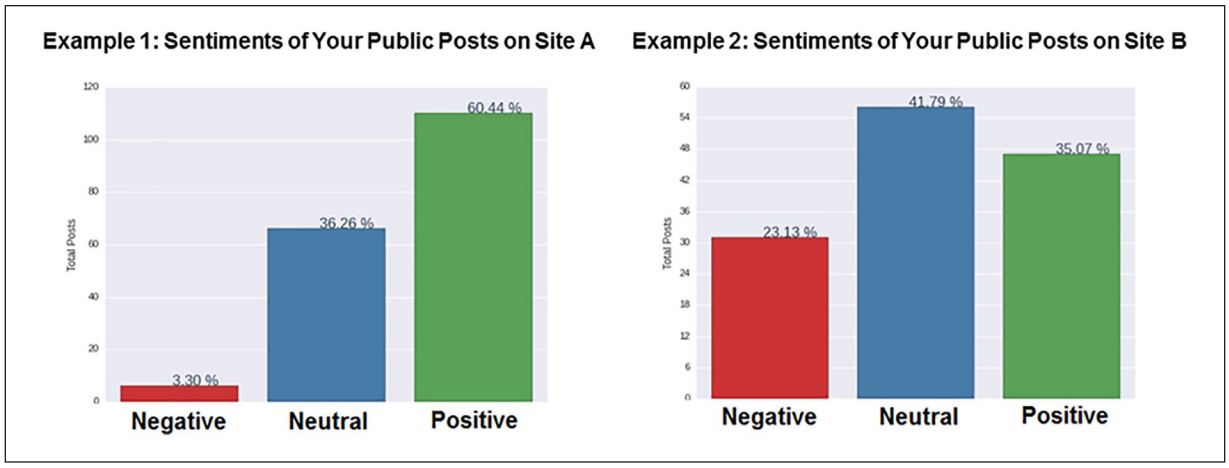

Figure 1. Sample visualization of sentiment.

Table 3. Constructs' Reliability and Validity.

Constructs	Internal consistency reliability			Convergent validity
	Cronbach's alpha	rho A	Composite reliability	Average variance extracted (AVE)
Recommended Threshold	⩾.7	⩾.7	⩾0.7	⩾0.5
COL	.866	.88	0.908	0.711
ERR	.829	.881	0.896	0.741
SUS-UAC	.868	.882	0.898	0.559
HRComf	.915	.922	0.931	0.66

COL: collection; ERR: errors; SUS-UAC: secondary use-unauthorized access.

that the seven information types can be used to create a unidimensional, composite comfort level score using the mean function.

The reliability and validity of the four constructs (COL, ERR, SUS-UAC, and HRComf) were assessed using four common tests: Cronbach's Alpha, rho A, Composite Reliability, and Average Variance Extracted (AVE). All values are within their recommended thresholds (Hair et al., 2017; Henseler et al., 2016) and confirm the adequacy of the measurement instrument (see Table 3).

A P-P plot and a distribution of residuals for the dependent variable (HRComf) supports the normality assumption of the residuals. Finally, we confirmed that there is no multicollinearity among the independent variables (all variance inflation factors (VIFs) <1.5, with the recommended threshold of 3).

Results

Participants' Demographics

Our sample is well balanced in terms of gender and job seeking status. Consistent with other AMT-based samples (Berinsky et al., 2012; Paolacci et al., 2010; Wang et al., 2011), our sample is skewed toward younger (but older than student samples; age group 25–34), more educated, social media users who use at least 1 of the 11 popular social media sites. The only major difference between our sample and those reported in other AMT-based studies is that we had a higher proportion of male participants—especially in the sample from India (see Table 4).

Automatic Linear Modeling

The resulting model (see Table 5) explains 17% of the total variance of the comfort level with employers' use of social media to screen job applicants.[3] The model shows that the *country* and *privacy concerns* factors are the strongest predictors of comfort level. In particular, the comfort score was higher for respondents from India, supporting that one's culture plays a role in the social media screening context (RQ1). However, neither *gender* (RQ2) nor one's *job seeking status* (RQ3) was included in the best performing model. The results for RQ4 were mixed. In this section, we review each of our research questions in turn.

RQ1 (Culture): Do People Living in India React to Cybervetting Differently Than Those in the United States? We found that

living in India is positively and significantly associated with being more comfortable with the practice of screening job applicants. Thus, Hypothesis 1 is supported. This finding could be as a result of the cultural and/or regulatory differences in the United States and India (Bellman et al., 2004), and also because in India "the social and family structures place much less importance on privacy" (Ion et al., 2011, p. 12).

RQ2 (Gender): Do Women React to Cybervetting Differently Than Men? Even though some previous work has suggested that women have a higher level of privacy concerns than men in the context of internet and social media use (Bartel Sheehan, 1999; Cho & Hung, 2011; Youn & Hall, 2008), our research evidences no significant relationship between one's gender and the comfort level with social media screening. Hence, Hypothesis 2 is not supported. This may be because we investigated the comfort level in the specific context of screening job applicants using social media. In this context, there may be some "universal" expectations and concerns regardless of one's gender. In a related study of employed and non-employed Italian job seekers, the researchers also found no gender-based difference between professional online image concerns and inappropriate self-disclosure (El Ouirdi et al., 2015). They proposed that this could be because career-oriented items in their study "included an implicit minimum disclosure threshold on social media, and that it is widely common to disclose this amount of information by default without necessarily being on the job market" (El Ouirdi et al., 2015, p. 9).

Table 4. Participant Background.

Demographic	*N* = 429	Percentage (%)
Gender		
Women	184	43
Men	245	57
Age		
Under 25	57	13
25–34	195	45
35–44	115	27
45–54	40	9
55–64	19	4
65 or older	3	1
Job Seeker (7-point Likert scale)		
Not likely (scores 1–4)	205	48
Likely (scores 5–7)	224	52
Education		
Some school, no degree	3	1
High school diploma	29	7
Some college, no degree	96	22
College diploma	51	12
Bachelor's degree	159	37
Master's degree	75	17
Professional degree (JD, MD, DO, etc.)	8	2
Doctorate degree	8	2
Country		
United States	316	74
India	113	26

RQ3 (Motivation): Do Job Seekers React to Cybervetting Differently Than Non-Job Seekers? This question focuses on whether there is a difference in reaction between job seekers and those who are not currently seeking or planning to seek employment in the near future to the practice of screening job applicants. The result shows that the likelihood of being on the job market is not associated with people's attitude toward social media screening; in other words, being a job seeker does not necessarily make one more or less comfortable with the practice. Therefore, Hypothesis 3 is not supported. The result emphasizes the need for employers and recruiters, who rely on social media to screen job applicants, to be aware that the practice may "reduce the attractiveness of an organization during various phases of the selection process, especially if the applicant pool at large knows or suspects that the organization engages in such screening" (Stoughton et al., 2015, p. 86).

RQ4 (Risk-Benefit Ratio): Is There a Relationship Between Users' Privacy Concerns on Social Media and Their Attitude Toward Cybervetting? The answer to this question is "yes,"

Table 5. Result of Automatic Linear Analysis.

Independent Variables	Coef.*	Std. Error	t	Sig.	Importance (effects)
Intercept	5.425	0.650	8.345	0.000	
Country = "India"	1.071	0.170	6.314	0.000	0.513
ERR	0.281	0.067	4.192	0.000	0.226
SUS-UAC	−0.431	0.114	−3.780	0.000	0.184
COL	−0.170	0.070	−2.435	0.015	0.076

COL: collection; ERR: errors; SUS-UAC: secondary use-unauthorized access.
*Only statistically significant coefficients are included in the table ($p \leq .05$).

but the sign of the relationship depends on the specific privacy concern. The comfort score in our model is negatively associated with two of three privacy-related factors: COL and SUS-UAC. This finding suggests that higher concerns with social media sites collecting personal information and possibly using/sharing such information without users' consent are both associated with a lower comfort level with organizations using social media data to screen job applicants—even if the social media data are publicly available.

At the same time, the comfort score is positively associated with the *ERR* privacy factor, which can be interpreted as people who are more comfortable with the use of social media to screen job applicants are also more concerned if social media sites store erroneous information about them. People could perceive that having incorrect information about themselves stored publicly on social media could negatively impact their prospect of being successful in the social media screening process. This suggests that the *ERR* factor in this social media screening context may be more related to one's image management concerns than privacy-related concerns.

In sum, Hypothesis 4 is generally supported, except when it comes to the *ERR* factor. This result may suggest the presence of a phenomenon called "digital resignation" (Turow et al., 2015). Digital resignation refers to the situation where people are generally concerned about privacy, but they also reluctantly recognize that companies would still engage in this practice regardless of their concerns—especially when it comes to using publicly available social media data. Thus, social media users may want to ensure that information collected about them from social media is at least accurate, as misleading erroneous representations of oneself may negatively impact an employer's hiring decision (e.g., if the data point to an applicant's lack of influence on social media). A similar concern of misrepresentation and misattribution of job applicants was identified by Frantz et al. (2016). The result indicates that this concern is especially important for people who are more comfortable with social media screening.

Conclusion

The hiring process requires trust from all stakeholders, yet employers have grown to distrust information that were conventionally sourced (Berkelaar, 2014). In a social media age, employers are now turning to cybervetting and the role of trust between these organizations and job seekers is being renegotiated. Our research investigates how job seekers and non-job seekers perceive the practice of prospective employers using publicly accessible social media data to screen job applicants. The results of the research can be broadly divided into the following two areas: (1) theoretical implications for privacy research and social media research and (2) practical implications for the human resources sector.

Theoretical Implications

CPM predicts that the five factors of culture, gender, motivation, risk-benefit ratio, and context would be influential in privacy considerations. We tested these factors within the context of organizations using social media for screening and found that culture and risk-benefit ratio (assessed through three dimensions of privacy concerns) have shown to be associated with one's concerns related to social media screening, but neither gender nor motivation (operationalized as one's job seeking status) were associated with concern with cybervetting.

As a contribution to the literature, we have extended the application of the CPM theory beyond the management of private information to analyze "private" information that is public. The results confirm that the "fuzzy boundaries" (Child & Starcher, 2016) of privacy management become even fuzzier with regard to private information that is publicly available—as is the case with social media. Importantly, our findings support the notion that privacy boundaries are not only important when it comes to private information, but also with information that is publicly available on social media.

A limitation of the study is the use of the study participants' geographic location as a proxy to overall cultural context they live in when testing RQ1. Since identifying the United States as an individualist culture and India as a collectivist culture is a simplification of cultural context, future research could incorporate Hofstede's cultural dimensions and related scales (Eringa et al., 2015; Hofstede & Bond, 1984) to enable a more accurate assessment of cultural values and differences at the individual level.

Another limitation of the research is that we did not collect information about uses and gratification factors that influence one's social media use more broadly, as these have also been shown to influence one's self-disclosure on social media (Bauer & Schiffinger, 2015) and may also influence one's attitude toward the studied practice. For example, people who are seeking employment opportunities and also are using social media to create a professional online presence may be highly comfortable with prospective employers accessing their publicly available social media data for job screening purposes. In our case, we only captured the first part of this condition: whether someone is likely to seek employment or not.

Implications for Organizational Human Resources

Both inside and outside of organizations, social media has had a transformative impact; however, we have "barely scratched the surface of what is coming and what is possible" (Aral et al., 2013, p. 3). In just a few years, the scholarly community has begun to dig deep into the impact of organizations using social media for purposes such as hiring. In

addition to the data management issues, the organizational practice of prospective employers using social media to research, screen, and vet job applicants without their explicit consent also raises equity and trust issues. While social media can be used to verify information on a person's resume, the practice also affords prospective employers an unprecedented opportunity to examine the personal lives of job applicants. Accordingly, in an attempt to bolster HR transparency in 2017, the European Union made a decision that requires companies to publicly identify and warn applicants if their job screening process involves social media screening (Schrieberg, 2017). Many states in the United States have also banned employers from asking job applicants for access to their social media accounts (Wright, 2014). This decision is aligned with the finding that people tend to have less privacy concerns when companies explicitly ask for permission to use their information (Nowak & Phelps, 1995).

Beyond the disclosure of information, the CPM theory outlines that when an individual shares private information with others, the receiver of that information takes on the responsibility of guarding that information (Petronio, 2002). Shifted to public social media, we contend that third parties who use social media data need to be held to a similar standard to guard the information. This is supported by the presence of a negative and significant association between privacy concerns related to SUS-UAC of social media data by third parties and people's comfort with screening job applicants on social media. This is also supported by the finding that a person's job seeking status does not necessarily make them more comfortable with cybervetting.

One of the strongest results in our research was that respondents from India were significantly more comfortable with the practice of social media screening than those living in the United States; the finding is aligned with some previous work on cultural and regulatory differences between the two countries (Kumaraguru et al., 2005). Finally, we did not find any differences in responses based on gender, which suggests that in the context of employment seeking, there may be some consistent set of norms, expectations, or "privacy rules" that apply—irrespective of one's gender.

The results of the study can help organizations develop best practices when relying on social media for screening purposes by providing a nuanced understanding of people's comfort with the practice. For example, organizations that conduct hiring in different countries or recruit people with different cultural or ethnic backgrounds should recognize that some cultures may be more or less comfortable with organizations using social media screening. Overall, the significance of the research is that it identifies that just because social media data are public, does not mean people do not have context-specific and data-specific expectations of privacy.

Acknowledgements

The authors would also like to thank Philip Mai for his help and feedback during the preparation of this article. Earlier iterations of this work have been presented at the 2017 Americas Conference on Information Systems and the 2017 Canadian Association for Information Science Conference.

Declaration of Conflicting Interests

The author(s) declared no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author(s) disclosed receipt of the following financial support for the research, authorship, and/or publication of this article: This research is supported in part through a 5-year initiative on "Social Media Data Stewardship" funded by the Canada Research Chairs program (2015–2020; Principal Investigator: Gruzd, A) and the Ted Rogers School of Management at Ryerson University.

ORCID iDs

Anatoliy Gruzd https://orcid.org/0000-0003-2366-5163
Jenna Jacobson https://orcid.org/0000-0002-1371-1077
Elizabeth Dubois https://orcid.org/0000-0003-1323-516X

Notes

1. We recognize that gender is not a binary category and rather exists upon a continuum. In the survey, people were asked to self-identify as male or female, and we gave the option of not disclosing.
2. As a best practice, researchers should aim to provide compensation on AMT that is equal to the minimum wage in the country where the research is being conducting. Setting the compensation rate for an international survey, however, is complex. In India, there are state-specific and category-specific minimum wages that widely range across the country, but are below US$1.00 per hour, whereas the US federal minimum wage is US$7.25. Driven by an attempt to leverage an ethical and equitable practice across the countries, we leaned toward the higher minimum wage.
3. We also tested the age group as one of the independent variables, but its inclusion only slightly improved the model (adjusted R^2 increased from .17 to .18); this model only accounted for 13 people of age 55+ whose comfort score was slightly lower relatively to other groups.

References

Altman, I., & Taylor, D. A. (1973). Social penetration: The development of interpersonal relationships. Holt, Rinehart & Winston.

Aral, S., Dellarocas, C., & Godes, D. (2013). Introduction to the special issue—Social media and business transformation: A framework for research. *Information Systems Research*, *24*(1), 3–13. https://doi.org/10.1287/isre.1120.0470

Barrick, M. R., Shaffer, J. A., & DeGrassi, S. W. (2009). What you see may not be what you get: Relationships among self-presentation tactics and ratings of interview and job performance. *Journal of Applied Psychology*, *94*(6), 1394–1411.

Bartel Sheehan, K. (1999). An investigation of gender differences in on-line privacy concerns and resultant behaviors. *Journal of Interactive Marketing*, *13*(4), 24–38. https://doi.org/10.1002/(SICI)1520-6653(199923)13:4<24::AID-DIR3>3.0.CO;2-O

Baruh, L., Secinti, E., & Cemalcilar, Z. (2017). Online privacy concerns and privacy management: A meta-analytical review. *Journal of Communication*, *67*(1), 26–53.

Batenburg, A., & Bartels, J. (2017). Keeping up online appearances: How self-disclosure on Facebook affects perceived respect and likability in the professional context. *Computers in Human Behavior*, *74*, 265–276. https://doi.org/10.1016/j.chb.2017.04.033

Bauer, C., & Schiffinger, M. (2015, January). Self-disclosure in online interaction: A meta-analysis. In *2015 48th Hawaii International Conference on System Sciences* (pp. 3621–3630). IEEE. https://doi.org/10.1109/HICSS.2015.435

Bauer, T. N., Truxillo, D. M., Tucker, J. S., Weathers, V., Bertolino, M., Erdogan, B., & Campion, M. A. (2006). Selection in the information age: The impact of privacy concerns and computer experience on applicant reactions. *Journal of Management*, *32*(5), 601–621. https://doi.org/10.1177/0149206306289829

Bellman, S., Lecturer, S., Johnson, E. J., Kobrin, S. J., Wurster, W. H., Management, P. M., & Lohse, G. L. (2004). International differences in information privacy concerns: A global survey of consumers. *The Information Society*, *20*(5), 313–324.

Berinsky, A. J., Huber, G. A., & Lenz, G. S. (2012). Evaluating online labor markets for experimental research: Amazon.com's Mechanical Turk. *Political Analysis*, *20*(3), 351–368. https://doi.org/10.1093/pan/mpr057

Berkelaar, B. L. (2014). Cybervetting, online information, and personnel selection: New transparency expectations and the emergence of a digital social contract. *Management Communication Quarterly*, *28*(4), 479–506. https://doi.org/10.1177/0893318914541966

Berkelaar, B. L., & Buzzanell, P. M. (2015). Online employment screening and digital career capital: Exploring employers' use of online information for personnel selection. *Management Communication Quarterly*, *29*(1), 84–113. https://doi.org/10.1177/0893318914554657

Buhrmester, M., Kwang, T., & Gosling, S. D. (2011). Amazon's Mechanical Turk: A new source of inexpensive, yet high-quality, data? *Perspectives on Psychological Science: A Journal of the Association for Psychological Science*, *6*(1), 3–5. https://doi.org/10.1177/1745691610393980

CareerBuilder. (2018). *More than half of employers have found content on social media that caused them NOT to hire a candidate, according to recent CareerBuilder survey*. http://press.careerbuilder.com/2018-08-09-More-Than-Half-of-Employers-Have-Found-Content-on-Social-Media-That-Caused-Them-NOT-to-Hire-a-Candidate-According-to-Recent-CareerBuilder-Survey

Cavusoglu, H., Phan, T. Q., Cavusoglu, H., & Airoldi, E. M. (2016). Assessing the impact of granular privacy controls on content sharing and disclosure on Facebook. *Information Systems Research*, *27*(4), 848–879. https://doi.org/10.1287/isre.2016.0672

Child, J. T., Haridakis, P. M., & Petronio, S. (2012). Blogging privacy rule orientations, privacy management, and content deletion practices: The variability of online privacy management activity at different stages of social media use. *Computers in Human Behavior*, *28*(5), 1859–1872. https://doi.org/10.1016/j.chb.2012.05.004

Child, J. T., & Starcher, S. C. (2016). Fuzzy Facebook privacy boundaries: Exploring mediated lurking, vague-booking, and Facebook privacy management. *Computers in Human Behavior*, *54*, 483–490. https://doi.org/10.1016/j.chb.2015.08.035

Cho, V., & Hung, H. (2011). The effectiveness of short message service for communication with concerns of privacy protection and conflict avoidance. *Journal of Computer-Mediated Communication*, *16*(2), 250–270. https://doi.org/10.1111/j.1083-6101.2011.01538.x

DeGroot, J. M., & Vik, T. A. (2017). "We were not prepared to tell people yet": Confidentiality breaches and boundary turbulence on Facebook. *Computers in Human Behavior*, 70, 351–359.

Dinev, T., Xu, H., Smith, J. H., & Hart, P. (2013). Information privacy and correlates: An empirical attempt to bridge and distinguish privacy-related concepts. *European Journal of Information Systems*, *22*(3), 295–316. https://doi.org/10.1057/ejis.2012.23

Dubois, E., Gruzd, A., & Jacobson, J. (2020). Journalists' use of social media to infer public opinion: The citizens' perspective. *Social Science Computer Review*, *38*(1), 57–74. https://doi.org/10.1177/0894439318791527

El Ouirdi, M., Segers, J., El Ouirdi, A., & Pais, I. (2015). Predictors of job seekers' self-disclosure on social media. *Computers in Human Behavior*, *53*, 1–12. https://doi.org/10.1016/j.chb.2015.06.039

Eringa, K., Caudron, L. N., Rieck, K., Xie, F., & Gerhardt, T. (2015). How relevant are Hofstede's dimensions for intercultural studies? A replication of Hofstede's research among current international business students. *Research in Hospitality Management*, *5*(2), 187–198.

Frantz, N. B., Pears, E. S., Vaughn, E. D., Ferrell, J. Z., & Dudley, N. M. (2016). Is John Smith really John Smith? Misrepresentations and misattributions of candidates using social media and social networking sites. In R. N. Landers & G. B. Schmidt (Eds.), *Social media in employee selection and recruitment* (pp. 307–339). Springer International Publishing. https://doi.org/10.1007/978-3-319-29989-1_15

Ghoshray, S. (2013). Emerging reality of social media: Erosion of individual privacy through cyber-vetting and law's inability to catch up. *John Marshall Review of Intellectual Property Law*, *12*, 551–582.

Goodman, J. K., Cryder, C. E., & Cheema, A. (2013). Data collection in a flat world: The strengths and weaknesses of mechanical Turk samples. *Journal of Behavioral Decision Making*, *26*(3), 213–224. https://doi.org/10.1002/bdm.1753

Gruzd, A., & Hernández-García, Á. (2018). Privacy concerns and self-disclosure in private and public uses of social media. *Cyberpsychology, Behavior, and Social Networking*, *21*(7), 418–428. https://doi.org/10.1089/cyber.2017.0709

Gruzd, A., Jacobson, J., & Dubois, E. (2017a). Information visualizations as a tool to study users' social media privacy concerns. In *Proceedings of the Annual Conference of CAIS/Actes Du Congrès Annuel de l'ACSI* (pp. 1–5). https://doi.org/10.29173/cais1016

Gruzd, A., Jacobson, J., & Dubois, E. (2017b, August). *You're hired: Examining acceptance of social media screening of job applicants*. AMCIS 2017 Proceedings, Boston, MA. https://aisel.aisnet.org/amcis2017/DataScience/Presentations/28

Gundecha, P., & Liu, H. (2012). Mining social media: A brief introduction. In P. B. Mirchandani (Ed.), *2012 TutORials in Operations Research* (pp. 1–17). INFORMS. https://doi.org/10.1287/educ.1120.0105

Hair, J., Hollingsworth, C. L., Randolph, A. B., & Loong Chong, A. Y. (2017). An updated and expanded assessment of PLS-SEM in information systems research. *Industrial Management & Data Systems*, *117*(3), 442–458. https://doi.org/10.1108/IMDS-04-2016-0130

Hauser, D. J., & Schwarz, N. (2016). Attentive Turkers: MTurk participants perform better on online attention checks than do subject pool participants. *Behavior Research Methods*, *48*(1), 400–407. https://doi.org/10.3758/s13428-015-0578-z

Hedenus, A., Backman, C., & Håkansson, P. (2019). Whom do you know? Recruiters' motives for assessing jobseekers' online networks. *The International Journal of Human Resource Management*, 1–24. https://doi.org/10.1080/09585192.2019.1579245

Henseler, J., Hubona, G., & Ray, P. A. (2016). Using PLS path modeling in new technology research: Updated guidelines. *Industrial Management & Data Systems*, *116*(1), 2–20. https://doi.org/10.1108/IMDS-09-2015-0382

Hofstede, G., & Bond, M. H. (1984). Hofstede's culture dimensions: An independent validation using Rokeach's value survey. *Journal of Cross-Cultural Psychology*, *15*(4), 417–433. https://doi.org/10.1177/0022002184015004003

Huberty, C. J. (1989). Problems with stepwise methods: Better alternatives. *Advances in Social Science Methodology*, *1*, 43–70.

Ion, I., Sachdeva, N., Kumaraguru, P., & Čapkun, S. (2011, July). Home is safer than the cloud!: Privacy concerns for consumer cloud storage. In *Proceedings of the Seventh Symposium on Usable Privacy and Security* (pp. 13:1–13:20). ACM. https://doi.org/10.1145/2078827.2078845

Jacobson, J., & Gruzd, A. (2020). Cybervetting job applicants on social media: The new normal? *Ethics and Information Technology*, 1–21. https://doi.org/10.1007/s10676-020-09526-2

Jacobson, J., Gruzd, A., & Hernández-García, Á. (2020). Social media marketing: Who is watching the watchers? *Journal of Retailing and Consumer Services*, *53*, Article 101774. https://doi.org/10.1016/j.jretconser.2019.03.001

Jeske, D., & Shultz, K. S. (2019). Social media screening and content effects: Implications for job applicant reactions. *International Journal of Manpower*, *40*(1), 73–86.

Kluemper, D. H., Rosen, P. A., & Mossholder, K. W. (2012). Social networking websites, personality ratings, and the organizational context: More than meets the eye? *Journal of Applied Social Psychology*, *42*(5), 1143–1172. https://doi.org/10.1111/j.1559-1816.2011.00881.x

Krasnova, H., Günther, O., Spiekermann, S., & Koroleva, K. (2009). Privacy concerns and identity in online social networks. *Identity in the Information Society*, *2*(1), 39–63. https://doi.org/10.1007/s12394-009-0019-1

Kumaraguru, P., Cranor, L. F., & Newton, E. (2005, September). Privacy perceptions in India and the United States: An interview study. In *The 33rd Research Conference on Communication, Information and Internet Policy* (*TPRC*) (pp. 23–25). https://pdfs.semanticscholar.org/fac2/36ff4a5210dd1c3909ce6c6e8274827aef27.pdf

Madera, J. M. (2012). Using social networking websites as a selection tool: The role of selection process fairness and job pursuit intentions. *International Journal of Hospitality Management*, *31*(4), 1276–1282. https://doi.org/10.1016/j.ijhm.2012.03.008

Malhotra, N. K., Kim, S. S., & Agarwal, J. (2004). Internet users' information privacy concerns (IUIPC): The construct, the scale, and a causal model. *Information Systems Research*, *15*(4), 336–355.

Mason, W., & Suri, S. (2012). Conducting behavioral research on Amazon's Mechanical Turk. *Behavior Research Methods*, *44*(1), 1–23. https://doi.org/10.3758/s13428-011-0124-6

Nissenbaum, H. (2009). *Privacy in context: Technology, policy, and the integrity of social life*. Stanford University Press.

Nissenbaum, H. (2018). Respecting context to protect privacy: Why meaning matters. *Science and Engineering Ethics, 24*(3), 831–852. https://doi.org/10.1007/s11948-015-9674-9

Nowak, G. J., & Phelps, J. (1995). Direct marketing and the use of individual-level consumer information: Determining how and when "privacy" matters. *Journal of Direct Marketing*, *9*(3), 46–60.

Ollington, N., Gibb, J., & Harcourt, M. (2013). Online social networks: An emergent recruiter tool for attracting and screening. *Personnel Review*, *42*(3), 248–265. https://doi.org/10.1108/00483481311320390

Osatuyi, B. (2015). Empirical examination of information privacy concerns instrument in the social media context. *AIS Transactions on Replication Research*, *1*(1), 1–14. http://aisel.aisnet.org/trr/vol1/iss1/3

Oshima, T., & Dell-Ross, T. (2016, October). *All possible regressions using IBM SPSS: A practitioner's guide to automatic linear modeling* [Conference session]. Georgia Educational Research Association Conference, *1*. https://digitalcommons.georgiasouthern.edu/gera/2016/2016/1

Paolacci, G., Chandler, J., & Ipeirotis, P. G. (2010). Running experiments on Amazon Mechanical Turk. *Judgment and Decision Making*, *5*(5), 411–419.

Patil, S., Kobsa, A., John, A., & Seligmann, D. (2010). Comparing privacy attitudes of knowledge workers in the U.S. and India. In *Proceedings of the 3rd International Conference on Intercultural Collaboration* (pp. 141–150). ACM. https://doi.org/10.1145/1841853.1841875

Peluchette, J., & Karl, K. (2008). Social networking profiles: An examination of student attitudes regarding use and appropriateness of content. *CyberPsychology & Behavior*, *11*(1), 95–97. https://doi.org/10.1089/cpb.2007.9927

Petronio, S. (2002). *Boundaries of privacy: Dialectics of disclosure*. State University of New York Press.

Quinn, K., & Papacharissi, Z. (2018). The contextual accomplishment of privacy. *International Journal of Communication*, *12*, 45–67.

Rand, D. G. (2012). The promise of Mechanical Turk: How online labor markets can help theorists run behavioral experiments. *Journal of Theoretical Biology*, *299*, 172–179. https://doi.org/10.1016/j.jtbi.2011.03.004

Root, T., & McKay, S. (2014). Student awareness of the use of social media screening by prospective employers. *Journal of Education for Business*, *89*(4), 202–206. https://doi.org/10.1080/08832323.2013.848832

Roulin, N. (2014). The influence of employers' use of social networking websites in selection, online self-promotion, and personality on the likelihood of faux pas postings. *International Journal of Selection and Assessment*, *22*(1), 80–87. https://doi.org/10.1111/ijsa.12058

Ruggs, E. N., Walker, S. S., Blanchard, A., & Gur, S. (2016). Online exclusion: Biases that may arise when using social media in talent acquisition. In R. N. Landers & G. B. Schmidt (Eds.), *Social media in employee selection and recruitment* (pp. 289–305). Springer International Publishing. https://doi.org/10.1007/978-3-319-29989-1_14

Schmidt, G. B., & O'Connor, K. W. (2016). Legal concerns when considering social media data in selection. In R. N. Landers & G. B. Schmidt (Eds.), *Social media in employee selection and recruitment* (pp. 265–287). Springer International Publishing. https://doi.org/10.1007/978-3-319-29989-1_13

Schrieberg, D. (2017). E.U. wants to restrict job applicants' social media background checks. *Forbes*. https://www.forbes.com/sites/davidschrieberg1/2017/07/13/e-u-wants-to-restrict-job-applicants-social-media-background-checks/

Serewicz, M. C. M., & Petronio, S. (2007). Communication privacy management theory. In B. Whaley & W. Samter (Eds.), *Explaining communication: Contemporary theories and exemplars* (pp. 257–273). Lawrence Erlbaum.

Sivertzen, A.-M., Nilsen, E. R., & Olafsen, A. H. (2013). Employer branding: Employer attractiveness and the use of social media. *Journal of Product & Brand Management*, *22*(7), 473–483. https://doi.org/10.1108/JPBM-09-2013-0393

Smith, S. A., & Brunner, S. R. (2017). To reveal or conceal: Using communication privacy management theory to understand disclosures in the workplace. *Management Communication Quarterly*, *31*(3), 429–446. https://doi.org/10.1177/0893318917692896

Stewart, K. A., & Segars, A. H. (2002). An empirical examination of the concern for information privacy instrument. *Information Systems Research*, *13*(1), 36–49. https://doi.org/10.1287/isre.13.1.36.97

Stoughton, J. W., Thompson, L. F., & Meade, A. W. (2013). Big five personality traits reflected in job applicants' social media postings. *Cyberpsychology, Behavior, and Social Networking*, *16*(11), 800–805. https://doi.org/10.1089/cyber.2012.0163

Stoughton, J. W., Thompson, L. F., & Meade, A. W. (2015). Examining applicant reactions to the use of social networking websites in pre-employment screening. *Journal of Business and Psychology*, *30*(1), 73–88. https://doi.org/10.1007/s10869-013-9333-6

Turow, J., Hennessy, M., & Draper, N. (2015). *The tradeoff fallacy: How marketers are misrepresenting American consumers and opening them up to exploitation*. https://www.asc.upenn.edu/sites/default/files/TradeoffFallacy_1.pdf

Wang, Y., Norice, G., & Cranor, L. F. (2011). Who is concerned about what? A study of American, Chinese and Indian users' privacy concerns on social network sites. In J. M. McCune, B. Balacheff, A. Perrig, A.-R. Sadeghi, A. Sasse, & Y. Beres (Eds.), *Trust and trustworthy computing* (pp. 146–153). Springer. https://doi.org/10.1007/978-3-642-21599-5_11

Waters, S., & Ackerman, J. (2011). Exploring privacy management on Facebook: Motivations and perceived consequences of voluntary disclosure. *Journal of Computer-Mediated Communication*, 17(1), 101–115.

Wright, A. D. (2014, August 12). More states ban social media snooping. *SHRM*. https://www.shrm.org/resourcesandtools/hr-topics/technology/pages/social-media-snooping.aspx

Wu, L. (2013). Social network effects on productivity and job security: Evidence from the adoption of a social networking tool. *Information Systems Research*, *24*(1), 30–51. https://doi.org/10.1287/isre.1120.0465

Yang, H. (2013). The case for being automatic: Introducing the Automatic Linear Modeling (LINEAR) procedure in SPSS Statistics. *Multiple Linear Regression Viewpoints*, *39*(2), 27–37.

Youn, S., & Hall, K. (2008). Gender and online privacy among teens: Risk perception, privacy concerns, and protection behaviors. *CyberPsychology & Behavior*, *11*(6), 763–765. https://doi.org/10.1089/cpb.2007.0240

Zide, J., Elman, B., & Shahani-Denning, C. (2014). LinkedIn and recruitment: How profiles differ across occupations. *Employee Relations*, *36*(5), 583–604. https://doi.org/10.1108/ER-07-2013-0086

Author Biographies

Anatoliy Gruzd (PhD, University of Illinois at Urbana-Champaign) is a Canada Research Chair, associate professor and research director of the Social Media Lab at Ryerson University's Ted Rogers School of Management in Toronto, Canada. Gruzd studies how social media use is changing the ways in which people and organizations communicate, connect and how these changes impact our society.

Jenna Jacobson (PhD, University of Toronto) is an assistant professor at Ryerson University's Ted Rogers School of Management and a Research Fellow at Ryerson's Social Media Lab in Toronto, Canada. Her research analyzes the use and implications of digital technologies in society—with a focus on social media, branding, and user behavior.

Elizabeth Dubois (PhD, University of Oxford) in an assistant professor at the Department of Communication and Faculty Member at the Centre for Law, Technology and Society, University of Ottawa, Canada. Her research focuses on political uses of digital media, media manipulation, and political opinion formation.