Ethics and Information Technology (2020) 22:175–195
https://doi.org/10.1007/s10676-020-09526-2

ORIGINAL PAPER

Cybervetting job applicants on social media: the new normal?

Jenna Jacobson[1] · Anatoliy Gruzd[1]

Published online: 2 March 2020

Abstract
With the introduction of new information communication technologies, employers are increasingly engaging in social media screening, also known as cybervetting, as part of their hiring process. Our research, using an online survey with 482 participants, investigates young people's concerns with their publicly available social media data being used in the context of job hiring. Grounded in stakeholder theory, we analyze the relationship between young people's concerns with social media screening and their gender, job seeking status, privacy concerns, and social media use. We find that young people are generally not comfortable with social media screening. A key finding of this research is that concern for privacy for public information on social media cannot be fully explained by some "traditional" variables in privacy research. The research extends stakeholder theory to identify how social media data ethics should be inextricably linked to organizational practices. The findings have theoretical implications for a rich conceptualization of stakeholders in an age of social media and practical implications for organizations engaging in cybervetting.

Keywords Stakeholder theory · Cybervetting · Social media · Social media screening · Job screening · Privacy · Young people

Introduction

Human resource (HR) managers have traditionally been required to do more with less resources—particularly in recent years (DiRomualdo et al. 2018). As one of the organizational responses to chronic under-resourcing (Berkelaar 2010) and technological advancements that have expanded the ability of employers to engage in employee surveillance (Ajunwa et al. 2017), businesses engage in so-called *cybervetting* as part of the hiring process. Cybervetting is a practice also known as "…Internet surveillance, social media background checks, social media screening, online screening, social media profiling, or Facebook fired" (Berkelaar and Harrison 2017, p. 1). Employers can engage in a simple Google search and locate social media profiles of a job applicant and may further proceed to engage in a more sophisticated analysis of their digital footprint across platforms. The number of organizations that are using social media to screen job applicants has dramatically risen; CareerBuilder (2018) found that the practice had increased from 11 to 70% in a decade. In this paper, we specifically focus on the use of social media data posted by a person or about a person to evaluate their job application; thus, we use *cybervetting* and *social media screening* interchangeably.

An organization's typical recruitment process includes: (1) engaging in a requirements analysis, (2) posting a job ad, (3) receiving and selecting desirable applications, and (4) making a final recruitment decision (Bizer et al. 2005). With the growing availability of online and social media data about the workforce, organizations' recruitment methods have evolved to include new types of data (Janta and Ladkin 2013). In particular, social media sources are now commonly consulted during the recruitment and hiring process in phases (3) and (4) as a filtering mechanism (Gandini and Pais 2017). New startups seeking to capitalize on the opportunity have emerged to offer fee-based social media screening services for employers and promise sophisticated technological screening to determine "fit" (including family histories), reveal negative attributes (such as drinking or sexual posts), and identify other risks that could jeopardize the company ("RiskAware" 2017).

✉ Jenna Jacobson
jenna.jacobson@ryerson.ca

Anatoliy Gruzd
gruzd@ryerson.ca

[1] Ted Rogers School of Management, Ryerson University, 350 Victoria Street, Toronto, ON M5B 2K3, Canada

More than half of the employers who use social media screening admit that they have *not* hired someone because of what they have found online (CareerBuilder 2014). Yet, there appears to be a large disconnect between this reality and people's perceptions of how common it is for social media to have a negative impact on one's hirability. For example, even though previous research confirms that young people have high awareness of employers' use of social media for screening (Hurrell et al. 2017), another study shows that only 2% of social media users think that their social media posts have caused them to get fired or not be hired (Smith 2015). More companies are engaging in social media screening and people's awareness of social media screening is growing, yet individuals still do not believe that their social media activities are impacting their employment, which masks the reality that people's livelihoods may be impacted because of this practice. The practice of cybervetting becomes even more significant for young people who are trying to position themselves in the workforce as they often struggle to find secure well-paid positions and enter the labour market.

Using stakeholder management theory, we investigate young people's concerns with their publicly available social media data being used in the specific context of job hiring. While previous research has analyzed job candidates reactions to potential employers asking for their social media login information (Drake et al. 2016; McEwan and Flood 2017), our research analyzes perceptions of privacy for social media data that is already public and, as such, does not require any login information to obtain. The research is contextually situated at the interplay of the necessity of hiring the best people with limited resources, the organizational response of engaging in social media job screening, and the individual response of people expressing concern. In particular, with the focus on the individual response, we follow prior research that suggests there may be a relationship between an individual's comfort with this growing practice and their gender (Peluchette and Karl 2008), job seeking status (Richey et al. 2017), social media use (Fogel and Nehmad 2009), and privacy concerns (Osatuyi 2015; Ellison et al. 2011). Thus, we ask:

> What is the relationship between young people's comfort with social media screening and their gender, job seeking status, social media use, and privacy concerns?

We will unpack and substantiate this research question further in the following sections on the theoretical foundation and hypotheses.

Theoretical framework

Social media and privacy

Social media are becoming ubiquitous and embedded into the daily lives of many people; Facebook has reached 2 billion users and Instagram has over 800 million users (Statistica 2017a, b). 94% of online Canadian adults have at least one social media account (Gruzd et al. 2018). The benefits of using and engaging on social media have been well observed and include using the platforms for entertainment, social relationship building and maintenance, information seeking, and self-presentation (Ellison et al. 2007; Quan-Haase and Young 2010; Whiting and Williams 2013).

A by-product of the large-scale adoption of social media is social media data mining. Publicly available social media data is largely free and available to be legally used for any purpose by third parties. While social media companies themselves have unfiltered access to all the data and interaction data that is provided to them, third parties similarly have extraordinary access to public social media data that can be collected and analyzed using APIs or through third-party data resellers, such as *Gnip* and *DataSift*, who harvest and neatly package the data. The data is used to gain perspective on human behaviour and human interaction (Helm 2018; Kennedy 2016), and can be leveraged by individuals, governments, and corporations for strategic benefit, such as marketing and human resources.

The insights from social media data have also been used to influence how people vote, as the recent Cambridge Analytica scandal has shown (Rosenberg and Dance 2018). But unlike Cambridge Analytica where data was mined, the focus of our study is on "publicly" available social media data. What constitutes information that is "public" has long been debated and has largely been situated around "reasonable expectations of privacy" (Tverdek 2008). In the current social media landscape, "public" social media is available to be mined, analyzed, and used. Therefore, a password protected Facebook group is considered private, whereas an open exchange on Twitter is considered public (Townsend and Wallace n.d.). The privacy setting not only impacts who can see the social media posts, but who can capture the data and surrounding metadata and transactional data. For example, when a person first creates a Twitter account, the tweets are public by default, which means that any other account—person, organization, or bot—can view, follow, and interact with that user.

Young people are widely recognized as being heavy users of social media (Chen and Cheung 2018; Hargittai 2010; Williams et al. 2012). As evidenced in the repeated declaration in the media that privacy is "dead," the overwhelming ethos in popular culture is that young people do not care about privacy. With the constant tweeting, posting, and snapchatting, how could a generation that is "obsessed" with social media be concerned about privacy? Often described as "digital natives" (Palfrey and Gasser 2010), this—loosely (and often poorly) defined—generation is made up of young people born into a world of technology with the accompanying assumption that they have the comfort, digital skills, and literacy needed to navigate it successfully. However, some scholarly research points to young people having significant and nuanced privacy concerns on social media (Bailey and Steeves 2015; Marwick et al. 2010; Regan and Jesse 2018).

The traditional approach to privacy assumes that rational actors understand the risks and benefits of disclosure, while engaging in logical decision-making regarding their privacy. Westin (2000) puts forward the traditionalist typology of privacy by identifying three categories of consumers based on their privacy concerns: fundamentalist (high concern), pragmatist (medium concern), and unconcerned (low concern). Sheehan (2002) expanded on earlier work by introducing a four-part typology of online users: unconcerned internet users, circumspect internet users, wary internet users, and alarmed internet users. Rather than merely focusing on the level of concern, Drennan et al. (2006) focused on the behavioural responses to privacy concerns and developed a three-part typology: privacy-aware, privacy-suspicious, and privacy-active types. Building on this scholarship, Burkell and Fortier (2016) identified three privacy types on Facebook: personal users (strongest privacy expectations), image controllers (less strong privacy expectations as they recognize Facebook content is meant to be shared), and relaxed displayers (lowest privacy settings).

While the traditional approach to privacy assumes a logical decision-making process or "privacy calculus," an understanding of the true costs and benefits of the decision are not only complex, but also context specific (Acquisti and Grossklags 2005; Litt 2012; Loh 2018). Given the spread of big data analytics, there is a need to think differently about privacy (Mai 2016) as it is impossible, or extremely difficult, for people to fully comprehend, or imagine, how the data is going to be used or could be used in the future. The value of social media data is not merely in analyzing the posts or photos, but in how the data is used and processed by third parties (Kennedy 2016), such as prospective employers. The pragmatic approach to privacy, or the rational consumer choice approach, is problematic as it puts the burden and responsibility on the individual to understand and decide what is the best privacy option for them (Draper 2016). Further, purely adopting the rational cost-benefit calculation of privacy would result in an oversimplification as it does not account for emotion (Lutz and Strathoff 2014; Stark 2016). Information type, context, and institution are important considerations in people's decision-making regarding what information to share (Marwick and Hargittai 2018). Nissenbaum's (2011) *contextual integrity* is a conceptual framework that outlines the importance of context (the data subject, the data sender, the recipient of the data, the information type, and the transmission principle) in personal information flows. It challenges some traditional conceptions of privacy, rejects the public versus private information dichotomy, and demands that the use of information be appropriate to the specific context. We embrace a contextual understanding of privacy (Nissenbaum 2011) by specifying the job hiring context and further considering different types of publicly available user data from social media that can be used for cybervetting.

Stakeholder theory

Stakeholder theory was introduced by R. Edward Freeman in his 1984 seminal book, *Strategic Management: A Stakeholder Approach*. Stakeholder theory suggests that corporate governance of organizations has a responsibility towards a broad spectrum of stakeholders, and corporations need to understand the context of their various stakeholder relationships (Berman and Johnson-Cramer 2016; Freeman 1984). With an explicit organizational commitment to ethics, this theory runs counter to traditional shareholder theories that do not recognizes the "plurality of values"; stakeholder theory contends that the interests of all groups—or stakeholders—that are, or can be, impacted by an organization need to be considered (Freeman 1984). Rather than serving a single purpose, stakeholder theory provides a framework that serves a range of purposes (Freeman et al. 2010): "Unlike economic theory which aims at prediction, stakeholder theory aims to guide managerial action" (Visser et al. 2010, p. 375). Clarkson (1995) defines stakeholders as "persons or groups that have, or claim, ownership, rights, or interests in a corporation and its activities, past, present, or future" (p. 106). Identification of stakeholders is largely divided into primary stakeholders—who have a formal, contractual, or official relationship with the corporation, such as employees and customers—and secondary stakeholders—everybody else influenced by the corporation (Gibson 2000). Stakeholder theory is becoming an academic field due to the extensive application of the theory in business and society, as well as in information and communication research, yet there is further social scientific work that is needed as much of the field has yet to be explored (Berman and Johnson-Cramer 2016) and critically applied using empirical data.

Young people have generally been neglected and overlooked in stakeholder theory (Ville 2014). Donaldson and Preston (1995) explicitly recognize job applicants as stakeholders—as demonstrated in their declaration that "potential job applicants, unknown to the firm, nevertheless have a stake in being considered for a job (but not necessarily to get a job)" (p. 85). However, prior research on potential job applicants has analyzed organizational attractiveness (Greening and Turban 2000; Tsai and Yang 2010; Turban and Greening 1997), but has largely neglected the perspectives on the hiring process itself. Job applicants exist in a liminal space of potentially becoming primary stakeholders, while being secondary stakeholders at the time of application. Notably, Stone and Stone-Romero (1998) state that people's expectation of privacy needs to be protected in the job application process; however, they do not conduct empirical research to identify job applicants' privacy needs and, importantly, they were writing pre-social media. Accordingly, the vast majority of research in stakeholder theory has not analyzed the perspective of prospective employees as stakeholders, and in particular, there is a dearth of research on young job applicants as stakeholders, and our research seeks to fill this gap.

While stakeholder theory can be approached from a descriptive perspective that explores how organizations interact with stakeholders or an instrumental perspective that emphasizes the business case for adopting stakeholder management, in this research, we adopt a normative perspective to stakeholder theory that identifies the treatment of stakeholders based on moral principles (Jawahar and McLaughlin 2001; Mellahi et al. 2010). The normative perspective considers how organizations treat people (Jones and Wicks 1999), which we extend to people's social media data. The normative perspective of stakeholder theory contends that organizations "ought to view the interests of stakeholders as having intrinsic value" (Jones and Wicks 1999, p. 209), which our research embraces by developing an understanding of the perspectives of young job applicants as stakeholders. Accordingly, we use stakeholder theory to specifically explore and deeply analyze job applicants' concerns with social media screening as a way to inform organizational business practices.

There is a growing area of research that has sought to develop definitional precision of stakeholder theory; however, there has been little emphasis on the inclusion of a new form of corporate data: social media data. By identifying the asymmetries of the current power relations between data producers (job applicants) and data consumers (hiring organizations), this research begins from a place of recognizing and validating young job applicants as valid stakeholders whose concerns need to be carefully considered in business operations—specifically job hiring practices.

Hypothesis development

Hypothesis 1

We begin by testing the relationship between gender[1] and comfort with social media screening. Previous research repeatedly indicates that women tend to be more risk averse (Finucane et al. 2000; Forsythe and Shi 2003) and have higher privacy concerns in both online and offline spaces (Garbarino and Strahilevitz 2004). This tendency is apparent across age groups: Youn and Hall (2008) found that girls have higher privacy concerns and perceive higher levels of risks than boys. In the context of location-based services, Mao and Zhang (2014) found significant gender differences with women being more aware of and concerned with privacy issues. Peluchette and Karl (2008) evidenced that women were more concerned than men with employers seeing information on their social networking sites. Well aligned with the current study, Hoy and Milne (2010) examined gender differences with online privacy and secondary use of information on Facebook amongst young people and found that, although concern was low amongst both women and men, women were more concerned about their privacy being invaded and they also had higher levels of privacy protection behaviours. While previous studies do not distinguish between publicly available or private social media data, we hypothesize that in the context of publicly available on social media:

H_1 Women will be less comfortable with social media screening in comparison to men.

Hypothesis 2

Next, we turn to examining people's job seeking status. In a crowded labour market, people can use social media to help them positively stand out (Richey et al. 2017). According to the privacy calculus theory (Dinev and Hart 2006), people engage in a decision-making process to identify the costs of disclosing information versus the risks. As such, we hypothesize that job seekers have more to gain from social media screening, so will, therefore, be more comfortable than non-job seekers:

H_2 Job seekers will be more comfortable with social media screening than those who are not on the job market.

[1] We would like to acknowledge that the authors recognize that gender is not binary. Unfortunately, we did not have a large enough sample of people who elected "Trans*, non-binary, two-spirit, genderqueer, other" to be included in the statistical model.

Hypothesis 3

A growing body of literature has explored the relationship between privacy and self-disclosure (Bazarova and Choi 2014; Chang and Heo 2014). Recognizing the public nature of the internet, Fogel and Nehmad (2009) contend that people who post information about themselves are "more comfortable with the possible risks of their information being seen by others" (p. 159). Furthermore, those who have a higher number of public accounts may be engaged in strategic impression management and self-presentation (Goffman 1959; Leary and Kowalski 1990). Previous research by Dubois et al. (2020) found that the number of social media accounts an individual has significantly predicts the perception towards third party use of social media. Increased use of digital media increases one's media literacy (Livingstone 2004), which means an individual may modify their social media behaviour to limit their risks, resulting in higher comfort with the practice (Couldry and Powell 2014). As such, we hypothesize:

H_3 The number of public social media accounts a person has will be positively associated with their comfort with social media screening.

Hypothesis 4

Concern for information privacy has been shown to negatively impact people's attitudes and practices on the internet more broadly, as well as specifically on social media. For example, people with higher privacy concerns are less likely to use social media platforms (Osatuyi 2015); they are less trusting of mobile advertising (Okazaki et al. 2009); and they share less online (Chennamaneni and Taneja 2015). As such, we hypothesize a negative relationship between a person's information privacy concerns in the context of social media use and their comfort with social media screening:

H_4 People with higher concern for social media information privacy will be less comfortable with social media screening.

Hypothesis 5

Doolin et al. (2005) found that having a previous negative experience with online shopping (or even hearing about another person's negative experience) is negatively correlated with one's online shopping activity. Similarly, Okazaki et al. (2009) found that mobile phone users who had a previous negative experience with information disclosure had higher privacy concerns. Also related, Debatin et al. (2009) found that users who reported having a privacy invasion were more likely to change their privacy settings. While we do not test the same relationship, research evidences previous negative experience impacts concern, and as such, we hypothesize that the higher prior negative experience the lower the comfort:

H_5 People who have experienced an invasion of privacy on social media will be less comfortable with social media screening.

Hypothesis 6

The final hypothesis tests the relationship between users' knowledge of their privacy setting and comfort with social media screening. Despite an individual's confidence in their ability to manage their privacy online, Suh and Hargittai (2015) found that there is a considerable lack of effectiveness in users' online privacy management as people often mistakenly share posts publicly. Similarly, Hargittai and Marwick (2016) found that young adults feel that they have little control over personal information that is posted online. People who are unsure of their privacy setting may have low digital literacy (Ellison et al. 2011). As such, we hypothesize:

H_6 People who have knowledge of their privacy settings will be more comfortable with social media screening.

Method

After receiving approval from the Institutional Research Ethics Board, we collected data using an online survey. The survey was open from January 21 to April 11, 2017 and drew participants from the pool of undergraduate students at a Canadian university who signed up for the Student Research Participant Pool. Participation in the study was completely voluntary and the data was completely anonymized. Each student respondent received extra course credit upon completion of the survey. "Appendix A" includes the survey instrument.

Demographic and social media use

The survey asked general demographic questions, such as age, gender, and location, as well as questions about general online activities, social media use, and self-reported internet skills. Importantly, the survey specifically asked participants to identify whether their social media accounts are "primarily public," "primarily private," or "unsure." The survey also asked questions about participants' awareness of social media misuse and asked participants to report whether they personally have been a victim of a data privacy violation.

Measuring information privacy concerns

As a baseline measure for information privacy concerns, the survey asked questions about social media users' attitudes regarding the use of their social media data by third parties. We relied on a 14-question construct of Concern for Social Media Information Privacy (CFSMIP) (Osatuyi 2015), which was built by adapting Stewart and Segars' (2002) widely accepted construct of Concern for Information Privacy (CFIP) to the context of social media use. One of the main reasons for using this particular construct is because it fits well with the study's focus on users' concerns about organizational threats of social media data use. CFSMIP (and CFIP) assesses four main dimensions: concerns about *collection* of social media data by third parties (COL1–4), concerns about potential *errors* in users' information stored by organizations (ERR1–3), *secondary use* of social media data by third parties (SUS1–3), and *unauthorized access* by third parties (UAC1–4). Since CFSMIP is a multi-dimension construct and each dimension is measured based on 3 or 4 questions, we needed to ensure that relevant questions loaded on their corresponding dimension and that the measurement instrument for each dimension was reliable. Based on the Principal Components Factor Analysis, we discovered three factors that explain privacy concerns: Collection (COL), Errors (ERR), and a combined factor of Secondary Use (SUS) and Unauthorized Access (UAC) (see "Appendix B"). Although Cronbach's Alpha, rho A, and Composite Reliability were within the acceptable thresholds for all dimensions (Henseler et al. 2016; Hair et al. 2017), the Average Variance Extracted (AVE) value for the combined dimension of SUS and UAC was below the 0.5 threshold; thus, we removed it from the subsequent analysis. The discriminant validity was within the acceptable range for all remaining dimensions. In sum, we proceeded with two independent variables to assess users' information privacy concerns on social media: COL (the mean of COL1–4) and ERR (the mean of ERR1–3).

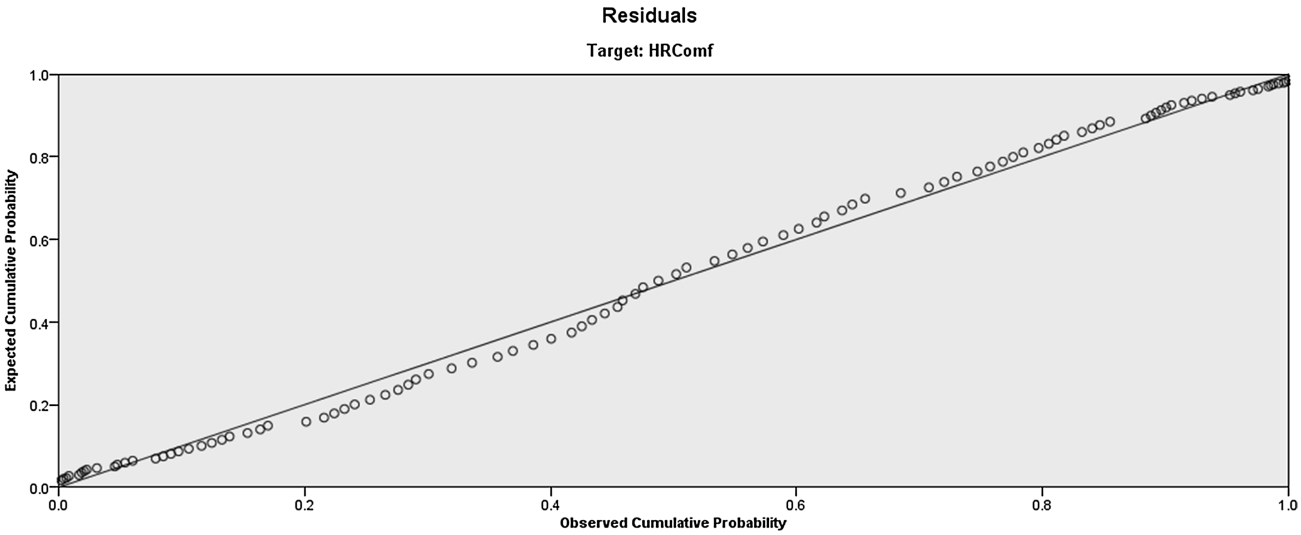
Measuring the comfort with social media screening (the comfort scale)

Prior research indicates that there is widespread knowledge of the practice of social media screening amongst young people (Hurrell et al. 2017); as such, the survey asked questions about students' attitudes toward their social media data being used by potential employers. These questions were used to construct the dependent variable as follows. To ensure that knowledge of social media screening did not act as a moderating variable, participants were shown a text-based brief that identified some of the common ways that prospective employers screen job applicants using social media. Participants were asked to assess their comfort level with a prospective employer accessing various types of their publicly available information on social media. The use of a 7-point comfort scale has been commonly and successfully adopted in privacy research (Lin et al. 2012; Lipford et al. n.d.; Schrodt 2013). Frye and Dornisch (2010) asked participants to rate their comfort disclosing information on various communication tools (e.g., email and instant messenger) and found that people were least comfortable disclosing information on public blogs and pages; Cranor et al. (1999) assessed people's comfort with providing specific pieces of information to websites and argued that the comfort level rises if users are informed and trust the disclosed policies. Comfort has been widely assessed and validated as a valuable construct in various contexts across disciplines (see Spake (2003) for a review). The evaluation of participants' comfort in combination with participants' concern has been adopted in online privacy and disclosure research (Spake et al. 2011).

In our study, we use both privacy concerns (as an independent variable) and comfort (as the dependent variable representing users' attitudes towards a particular practice). Privacy concerns were used as a baseline measure of individuals' concerns with organizations' use of social media more broadly—irrespective of data type and context. The comfort scale measured individuals' perceptions of specific data types in the specific context of job hiring and has been developed and evaluated by previous research (Gruzd et al. 2017; Jacobson and Gruzd 2018; Gruzd et al. in press). As the results of the research will indicate, the relationship between comfort and concern was weak, which confirms that these are indeed measuring different constructs.

As stated above, we specifically focused on information contributed by a user or by others on social media that is publicly available; in other words, such information has to be publicly accessible on social media platforms by others on the internet. In particular, we asked participants about nine different information types including: posts, photos, geolocation, frequent words, post frequency, sentiment, top posters (identification of the most prolific social media users), followers, and communication network. All questions were prefaced with a statement that asserted that only publicly available information is used (e.g. "Imagine that the following are your posts that show what you are saying on social media publicly.") Using a 7-point Likert scale where 1 = uncomfortable and 7 = comfortable, participants were asked, "How comfortable would you be if an employer uses information from social media about you to make a hiring decision?".

In an attempt to remove a potential bias in how participants perceived the social media information type questions, participants were randomly assigned to two groups where one group was shown text-based questions (n = 250), while the other group was shown visual-based questions (n = 232). For the purposes of this paper, we only focus on three information types: posts, photos, and top posters as there was no



The P-P plot of Studentized residuals compares the distribution of the residuals to a normal distribution.The diagonal line represents the normal distribution.The closer the observed cumulative probabilities of the residuals are to this line, the closer the distribution of the residuals is to the normal distribution.

Fig. 1 P–P plot of studentized residuals for the dependent variable (HRComf)

difference in participants' responses after viewing the visual-based versus the text-based question—as measured based on the Independent-Samples Median Test and Mann–Whitney U Test (see "Appendix C").

In summary, the dependent variable (HRComf) was calculated as the mean of the three comfort level questions: top posters (TopPostersComfort), posts (TweetComfort), and photos (MediaComfort). The reliability and validity of the new construct was assessed using Cronbach's Alpha (0.79), rho A (0.80), Composite Reliability (0.87), and Average Variance Extracted (0.70). All values were within their recommended thresholds and confirm the adequacy of the measurement instrument.

Data cleaning

In total, we received 556 survey responses. We cleaned the survey dataset by removing 25 responses by people who completed the survey twice (as the survey was open for several months, some participants may have forgotten that they completed the survey as some responses were two months apart). The "trap" question (attention check) asked, "Please select 'strongly agree' as your answer choice," and was inserted to screen participants who were not carefully reading the questions. We removed 42 survey responses that provided an incorrect answer to the trap question. We further removed 7 survey responses that had a completion time of less than 3 min in order to ensure a high quality of data responses. In total, after data cleaning, our dataset was comprised of 482 responses. The median completion time was 7 min and 44 s, and the mean completion time was 15 min and 29 s.

Data analysis

To test the proposed hypotheses, we used SPSS Version 24, statistical analysis software, to perform a linear regression using Automatic Linear Modeling (LINEAR) (Yang 2013). The model building method was "Best Subsets" using the Adjusted R Square criterion to select the best performing model identified by the highest adjusted R^2. By comparing all possible models (Oshima and Dell-Ross 2016), the best subsets method avoids a potential bias by not selecting the order of variable entry (Huberty 1989). The resulting regression model tested whether the comfort level (HRComf) can be predicted by any of the following independent variables: *Demographics*: (1) gender and (2) employment seeking status; *Social media use*: (3) number of public accounts; *Privacy concerns*: (4) COL, (5) ERR, (6) previous negative experience, and (7) number of "unsure in privacy settings" accounts.

A P–P plot of residuals for the dependent variable (HRComf) supports the normality assumption of the residuals (see Fig. 1). Finally, we confirmed that there is no multicollinearity among the independent variables (all VIFs, variance inflation factors < 1.15, within the recommended threshold of 3).

Results

Study participants

In terms of demographics, 65.1% of our survey participants self-identified as women (314 participants), 34.2%

Table 1 Participant demographics

	N = 482	Percentage (%)
Gender		
Women	314	65.1
Men	165	34.2
Trans*, non-binary, two-spirit, genderqueer, other	2	0.4
Prefer not to say	1	0.2
Age		
Under 25	448	92.9
25–34	30	6.2
35–44	2	0.4
45–54	1	0.2
55–64	0	0.0
65 or older	1	0.2
Prefer not to say	1	0.2

Table 2 Employment

	N = 482	Percentage (%)
Full-time	27	5.6
Unemployed	163	33.8
Part-time	282	58.5
Self-employed	10	2.1
Job seeking status[a]		
Unlikely (score 1–4)	136	28.2
Likely (score 5–7)	346	71.8

[a] Transformed variable from a 7-point Likert scale

as men (165 participants), 0.4% as "trans* non-binary, two-spirit, genderqueer, other" (2 participants), and 1 participant elected not to disclose (See Table 1). 92.9% of the participant pool was under 25 years old (448 participants) and 90% identified that they were from Canada, which is to be expected considering that the participant pool was comprised of undergraduate students enrolled at a Canadian university.

In terms of employment, the majority of students engaged in some form of work during their higher education: 58.5% worked part time, 5.6% worked full time, and 2.1% were self-employed (See Table 2). 71.8% of participants were job seekers, which is defined as an individual that is likely to seek employment within the next 6 months.

Social media use

Participants were active social media users with 63.3% (n = 305) using at least one social media platform on a daily basis or more frequently. Participants had a presence on an average of six social media platforms. The top platforms by popularity were Facebook (97%), Instagram (92%), Snapchat (92%), YouTube (82%), Twitter (74%), and LinkedIn (64%) (see Fig. 2). The majority of participants (71.6%) have not experienced an invasion of privacy on social media (see Table 3).

Privacy settings

Social media platforms present a range of privacy settings, and individual users can elect their privacy setting at the platform level. While an individual may have a public setting on a particular social media platform, the affordances of many platforms are such that one can elect to engage in private activities even if one's account is public. For example, an individual can elect to send a private message on Twitter even if their privacy setting is public. Similarly, a person with a private Facebook account can choose to create a public post or have some types of information public, while others are only accessible to friends. Accordingly, we elect to use the terms "primarily public" and "primarily private" to account for the ways people actually use the platforms, rather than creating an arbitrary, and inaccurate, binary.

Of the average of six social media platforms that participants had a presence on, three were primarily public and three were primarily private; therefore, prospective employers would be able to access the data from an average per person of three social media platforms that are publicly available—and this is not even considering various techniques to access information from private online spaces via requesting users' password, paying for targeted ads, tracking cookies from a web browser, and other approaches. Our participants tend to have public setting on the majority of sites, including: Own Blog/Website (81.7%), LinkedIn (71.7%), Tumblr (70.8%), Twitter (60.7%), and Pinterest (59.5%). Participants tend to have private accounts on Facebook (82.7%), Snapchat (78.1%), and Instagram (60.7%). The distribution is relatively even on Reddit (50.0%), Meetup (45.5%), and YouTube (43.2%) (See Table 4).

Fig. 2 Use of the most popular social media platforms

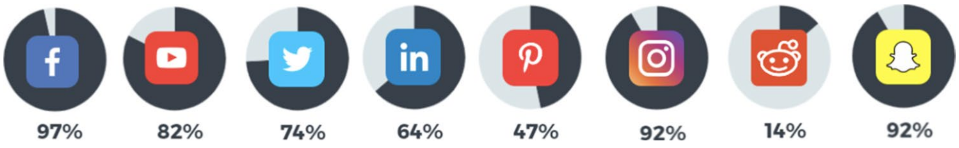


Table 3 Privacy victim

	n = 482	Percentage (%)
Yes	137	28.4
No	345	71.6

Table 4 Private vs. public social media use

	Public (%)	Private (%)	Unsure (%)
Facebook	16.0	82.7	1.3
Snapchat	16.6	78.1	5.3
Instagram	39.0	60.7	0.2
YouTube	43.2	44.0	12.8
Meetup	45.5	18.2	36.4
Reddit	50.0	35.9	14.1
Pinterest	59.5	24.3	16.2
Twitter	60.7	35.6	3.7
Tumblr	70.8	21.4	7.8
LinkedIn	71.7	19.4	8.9
Blog/Website	81.7	14.1	4.2

Table 5 Knowledge of privacy settings

	n = 482	Percentage (%)
0 unsure privacy setting	355	73.7
1 unsure privacy setting	83	17.2
> 1 unsure privacy setting	44	9.1

Privacy uncertainty

While 73.7% (n = 355) of students knew the privacy setting on all their social media platforms, 26.3% of students (n = 127) did not know the privacy setting on at least one of their social media accounts (See Table 5). Of those who did not know the privacy setting on at least one of their platforms, 65.4% (n = 83) did not know their privacy setting on one social media platform, and 34.6% (n = 44) did not know their privacy setting on more than one platform.

Information type comfort

To assess people's comfort level with their social media data being used by prospective employers, we identified three different social media data types: (1) Posters, referring to the most prolific users who posted in a public group/page on social media, had a mean comfort of 4; (2) Posts, referring to users' public text-based posts on social media, had a mean comfort of 4; and (3) Photos, referring to users' public visual-based posts on social media, had a mean comfort of 3. As expected, participants have a lower comfort with photos being used in social media screening in comparison to text-based social media posts (see Table 6). Depending on the data type, between 41.7 and 53.1% of participants are uncomfortable with social media screening.

Hypotheses testing

The resulting model (see Table 7) explains only 4.3% of the total variance of the comfort level with employers' use of social media to screen job applicants. This is important as it suggests that some factors that have been previously identified in the literature (such as gender, job seeking status, the number of social media accounts used, and knowledge of privacy settings) do not generally translate very well to publicly available social media data. Given the results of the regression model, we reject H_1 (gender), H_2 (job seeking status), H_3 (number of public social media accounts), and H_6 (knowledge of privacy settings), and accept H_4 (information privacy concerns, but only partially) and H_5 (previous negative experience).

On the one hand, young people's comfort with prospective employers using their social media data for job screening cannot be explained by demographic variable of gender. Women were not found to have higher privacy concerns at a statistically significant level. Aligned with Bergström's (2015) finding that there was no significant difference for privacy concerns amongst men and women in Sweden, this may suggest that women are engaging in pre-emptive privacy protection behaviours (Hoy and Milne 2010), or are managing their privacy for employment-related audiences (Hargittai and Litt 2013) and, as such, do not have higher concerns. Also, people's job seeking status, the number of public social media accounts, nor knowledge of their privacy settings can explain their comfort or discomfort with the studied practice.

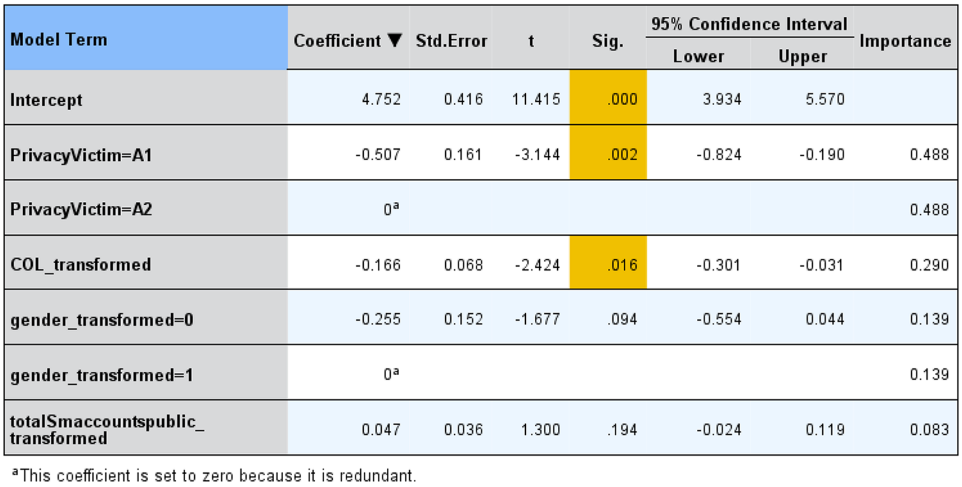
On the other hand, young people's comfort with prospective employers using their social media data for job screening is partially explained by their concern for social media

Table 6 Comfort with social media screening[a]

	Uncomfortable (1–3)	Neither comfortable, nor uncomfortable (4)	Comfortable (5–7)	Mean (1–7)
Posts	239 (49.6%)	76 (15.8%)	167 (34.6%)	3.60
Posters	201 (41.7%)	88 (18.3%)	193 (40.0%)	3.88
Photos	256 (53.1%)	76 (15.8%)	150 (31.1%)	3.44

[a] Transformed variable from a 7-point Likert scale where 1–3 = Uncomfortable, 4 = Neither comfortable, nor uncomfortable, and 5–7 = Comfortable

Table 7 Result of automatic linear analysis



Model Term	Coefficient ▼	Std.Error	t	Sig.	95% Confidence Interval		Importance
					Lower	Upper	
Intercept	4.752	0.416	11.415	.000	3.934	5.570	
PrivacyVictim=A1	-0.507	0.161	-3.144	.002	-0.824	-0.190	0.488
PrivacyVictim=A2	0^a						0.488
COL_transformed	-0.166	0.068	-2.424	.016	-0.301	-0.031	0.290
gender_transformed=0	-0.255	0.152	-1.677	.094	-0.554	0.044	0.139
gender_transformed=1	0^a						0.139
totalSmaccountspublic_ transformed	0.047	0.036	1.300	.194	-0.024	0.119	0.083

[a]This coefficient is set to zero because it is redundant.

The suffix "transformed" in COL, Gender, and TotalSMaccountsPublic indicates that the Automatic Linear Modeling (ALM) procedure automatically trimmed outliers by setting them to a cut-off value of three standard deviations from the mean for each of these variables. The "A1" value of the PrivacyVictim variable corresponds to the "yes" answer. Unsure variables were not included in the final model, as their inclusion did not improve the Adjusted R^2 square

information privacy: there is a statistically significant and negative relationship between Collection and young people's comfort with social media screening (people who are more concerned with their data being collected by social media platforms and third parties are less comfortable with cybervetting), but not between comfort and Error. Also, people who had experienced an invasion of privacy were also less comfortable with cybervetting.

Discussion

This research contributes to our understanding of users' ever-changing privacy expectation for publicly available social media data. We found that there is a relationship between comfort and one of the privacy concerns (COL) and having a previous negative experience, but many of the other factors previously identified in the privacy research were not applicable—including gender, job seeking status, social media use, and knowledge of privacy setting. This may suggest that there are other, or new, variables that need to be considered. Furthermore, considering that publicly available data comes from various social media platforms, the research sought to develop a cross-platform understanding of people's comfort with cybervetting. There may, however, also be platform-specific privacy concerns; for example, young people may use some social media platforms for purposeful professional reputation management (e.g., LinkedIn), while other platforms could be used for personal reasons and socialization which young people are not comfortable having used for cybervetting—even though the information is publicly available.

Although most of the factors that were tested in the regression model were not significant and the overall explanatory power of the model was very low (adjusted R^2 of 0.043), it does not mean that young people are comfortable with the practice of social media screening; in fact, about half of the participants were *not* comfortable with their publicly available social media data being used for social media screening; for example, 49.6% were uncomfortable with their public posts being used.

One of the results related to job seeking status is especially relevant in the context of stakeholder theory that was used to guide this study. With a commitment to organizational ethics, stakeholder theory contends that organizations have an explicit responsibility towards a spectrum of stakeholders including job applicants. As such, organizations cannot assume that people are comfortable with cybervetting—even if they are on the job market. This conclusion is also supported by the fact that 26.3% of participants do not know the privacy setting of at least one of their social media accounts, which speaks to the need for further social media data literacy at the individual and organizational levels. Organizations need to be cognizant of the fact that prospective employees might not intentionally share the information publicly.

The use of digital technologies in the workplace reconfigures work and employment (Howcroft and Taylor 2014), which introduces both opportunities and risks for employers and employees (Archer-Brown et al. 2018). The introduction of new technologies in the workplace has afforded increased organizational control (Pedersen et al. 2014). The practice of employers seeking to surveil and control their employees is not new as workplace surveillance has sought to improve worker efficiency and deter workplace misconduct (Ajunwa et al. 2017). These organizational practices can be met by worker resistance (Bain and Taylor 2000) and negative reactions by employees (Ball and Margulis 2011; Jeske and Santuzzi 2015). There is a clear incentive for employers to align their organizations' ethics with young people's expectations: organizations will be able to attract and keep these young employees (Weber 2017). If job applicants are aware of and not comfortable with an organization's social media screening practices then applicants may elect not to apply to the organization, and the organization may, consequently, lose the opportunity to recruit high-quality applicants. Alternatively, employees may lose trust in an organization if they later learn about the social media screening, which may similarly impact an organization's ability to recruit and retain the best candidates.

Further, organizations engaging in social media screening may open themselves up to claims of discriminatory hiring. Hiring is not a value-free and neutral process whereby the "best" applicant is offered the job; hiring discrimination has been well documented based on gender (Petit 2007), sexual orientation (Horvath and Ryan 2003), weight (Agerström and Rooth 2011), ethnic and racial identity (Derous et al. 2009), disability (Gouvier et al. 2003), mental health (Krupa et al. 2009), and so forth. Hiring discrimination is further compounded with people's intersectional identities, such as being a woman with a disability (O'Hara 2004). In addition to the existing forms of hiring discrimination that can be compounded, new forms of discrimination could emerge with social media screening, such as influence detection (whereby a lack of network influence is detrimental) or the introduction of predictive analytics (such as using photo filters to predict mental health).

Clark and Roberts (2010) have argued that "online character checks" harm society (p. 514) and conclude, "Rather than expecting users of SNSs [Social Networking Sites] to change their behavior by not posting anything they do not want an employer to view, we argue that it is better for society for employers not to enter an employee's virtual front door" (p. 519). With public social media data, the door is wide open, and individuals seeking employment do not know who has entered, what was gathered, and what assumption was made based on what was found. We contend that if organizations are to recognize job applicants as stakeholders, then they also need to recognize job applicants' concerns with social media job screening. More specifically, social media data ethics needs to be included in organizations' corporate social responsibility agendas and ethical corporate governance. One way for organizations to accomplish this is for transparency to be built into the hiring process and for organizations to clearly state their screening process.

There is a move towards regulating the job hiring process; for example, in 2017, the European Union's advisory body issued new guidelines that recommend barring employers from compiling social media data during the job hiring process unless it is "necessary and relevant" and further requiring employers to disclose if they are going to engage in cybervetting (Article 29 Data Protection Working Party 2017). Despite the lack of, or limited, laws that prescribe acceptable use of this practice, as a proactive step towards self-regulation, employers should clearly declare if they engage in cybervetting and specifically outline what social media platforms will be examined during the hiring process. In a move towards more ethical hiring practices, we recommend that employers allow job applicants to self-declare the social media accounts they would like to include as part of their job application.

Conclusion

In this paper, we embraced stakeholder theory to analyze young people's concerns with social media job screening to recognize job applicants as stakeholders and to inform organizational practices. Our research evidences that about half of the study participants were generally not comfortable with the practice of social media screening. We also found that the variables that have previously been identified in the privacy literature do little to explain this. Overall, the findings speak to the complexity and nuanced nature of individuals' understanding and perception of employers using social media data for job screening. As such, we argue that business ethics in the twenty-first century need to include considerations of job applicants' social media data privacy. We hope the research can guide managerial action in adopting appropriate ethical policies and processes for social media job screening, as outlined in stakeholder theory.

Our research supports the scholarship that suggests that ethics must be considered even if the data is public (Boyd and Crawford 2012). While individuals may indeed be posting publicly on social media, there is no way of fully comprehending how the data is, or can be, used now and in the future. Beyond a simple review of social media posts, social media analytics can be employed to analyze the public data in ways unbeknown to the original author. While the use of predictive analytics in social media—such as using social media posts to detect depression (Shen et al. 2017)—have begun to emerge, organizations and society need to be vigilant to ensure that the power relations do not become so unbalanced and unfair that job applicants are no longer considered stakeholders.

There are a few limitations to this research. The sample size of 482 students at one Canadian university limits the generalizability of findings that can be applied to a broader population. The quantitative data collection of this research does not afford an understanding of why people are comfortable or uncomfortable with the practice of social media screening. We encourage future work to continue this line of research using different user populations and methods, such as interviews or focus groups, to develop a nuanced understanding of the possible motivations and rationales. Furthermore, the survey did not use participants' own data for various reasons: (1) to not add uncontrollable variables that could influence the results, (2) to protect participants' privacy, and (3) to ensure participants considered all of their social media, rather than a sample, as this is what recruiters are able to access. If participants were shown their own data then the results may differ; for example, an individual may see a photo that they would be particularly embarrassed by.

To extend the findings of this research, future work could identify if and how young people are engaging in impression management practices on social media to determine if they purposefully adopt positive self-presentation strategies: do those who are comfortable with social media job screening employ careful self-censorship and impression management strategies to strategically foster a positive first impression on social media for employers? In addition, future work could analyze whether social media use is a mediator of comfort with this practice.

Acknowledgements An earlier version of this work appeared in the 2018 Academy of Management Conference Proceedings.

Funding This research is supported through a five-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.

Appendix A: Survey instrument

See Tables 8, 9, and 10

Table 8 Social media use and demographic questions

Social media use questions	
Social media use	Do you have an account on the following social media sites: Facebook [Yes; No; Unsure] LinkedIn [Yes; No; Unsure] Instagram [Yes; No; Unsure] Twitter [Yes; No; Unsure] Snapchat [Yes; No; Unsure] Tumblr [Yes; No; Unsure] YouTube [Yes; No; Unsure] Reddit [Yes; No; Unsure] Pinterest [Yes; No; Unsure] Meetup [Yes; No; Unsure] Your own blog/website [Yes; No; Unsure]
Privacy setting	What is the privacy setting of your social media account(s)? [Primarily PRIVATE; Primarily PUBLIC; Unsure]
Frequency	How often do you post on the following social media sites? [Never; Less than monthly; Monthly; Weekly; Daily; Several times a day; Unsure]
Privacy invasion	Have you personally been the victim of what you felt was an invasion of privacy on social media? [Yes; No]
Misuse exposure	Within the last year, how often have you encountered stories or examples of the potential misuse of social media data? [Never; Less than one per month; Monthly; Weekly; At least one a day]
Demographic questions	
Employment seeking	How likely are you to seek employment within the next 6 months? [Likert 1–7; 1 = Unlikely and 7 = Likely]
Employment status	Are you currently employed? [Full-time; Part-time; Self-employed; Not employed]
Age	What is your age group? [Under 25; 25–34; 35–44; 45–54; 55–64; 65 or older; Prefer not to say]
Gender	For the purposes of this study, how would you like to be identified? [Female; Male; Trans*, non-binary, two-spirit, genderqueer, other; Prefer not to say]
Education	What is the highest level of education earned? [Some school, no degree; High school graduate; Some college, no degree; College diploma; Bachelor's degree; Master's degree; Professional degree (J.D., M.D., D.O., etc.) Doctorate degree]
Country	Within the past 10 years, what country have you lived in the longest? [List of 171 countries]

Table 9 Concern for social media information privacy (CFSMIP)

To what extent do you agree with the following statements: *(7-point agreement/disagreement Likert 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	Computer 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

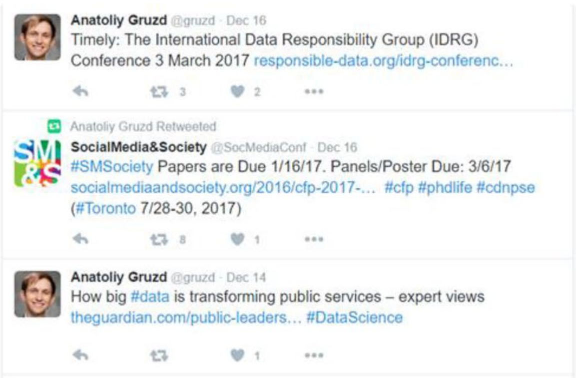
Adopted from Osatuyi (2015), and Stewart and Segars (2002)

Table 10 Comfort scale questions

How comfortable would you be if an employer uses this information about you to make a hiring decision? [Likert scale 1–7; 1 = uncomfortable, 7 = comfortable]

Posts

Example 1: Your Recent Social Media Posts

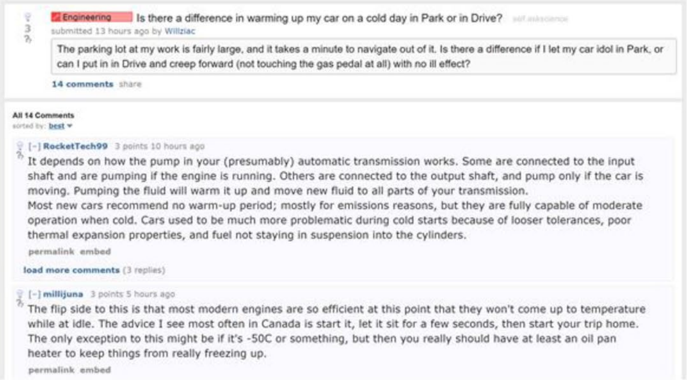


Anatoliy Gruzd @gruzd · Dec 16
Timely: The International Data Responsibility Group (IDRG) Conference 3 March 2017 responsible-data.org/idrg-conferenc…
3 2

Anatoliy Gruzd Retweeted
SocialMedia&Society @SocMediaConf · Dec 16
#SMSociety Papers are Due 1/16/17. Panels/Poster Due: 3/6/17 socialmediaandsociety.org/2016/cfp-2017-… #cfp #phdlife #cdnpse (#Toronto 7/28-30, 2017)
8 1

Anatoliy Gruzd @gruzd · Dec 14
How big #data is transforming public services – expert views theguardian.com/public-leaders… #DataScience
1

Example 2: Your Comments on a Public Forum



3

Engineering Is there a difference in warming up my car on a cold day in Park or in Drive?
submitted 13 hours ago by Willziac

The parking lot at my work is fairly large, and it takes a minute to navigate out of it. Is there a difference if I let my car idol in Park, or can I put in in Drive and creep forward (not touching the gas pedal at all) with no ill effect?

14 comments share

All 14 Comments
sorted by: best

[–] RocketTech99 3 points 10 hours ago
It depends on how the pump in your (presumably) automatic transmission works. Some are connected to the input shaft and are pumping if the engine is running. Others are connected to the output shaft, and pump only if the car is moving. Pumping the fluid will warm it up and move new fluid to all parts of your transmission.
Most new cars recommend no warm-up period; mostly for emissions reasons, but they are fully capable of moderate operation when cold. Cars used to be much more problematic during cold starts because of looser tolerances, poor thermal expansion properties, and fuel not staying in suspension into the cylinders.
permalink embed

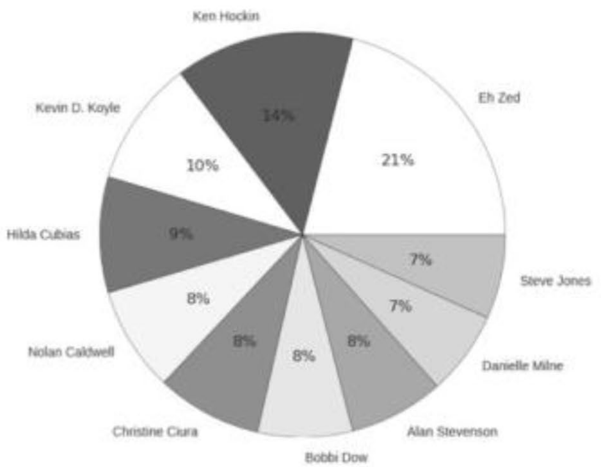
load more comments (3 replies)

[–] millijuna 3 points 5 hours ago
The flip side to this is that most modern engines are so efficient at this point that they won't come up to temperature while at idle. The advice I see most often in Canada is start it, let it sit for a few seconds, then start your trip home. The only exception to this might be if it's -50C or something, but then you really should have at least an oil pan heater to keep things from really freezing up.
permalink embed

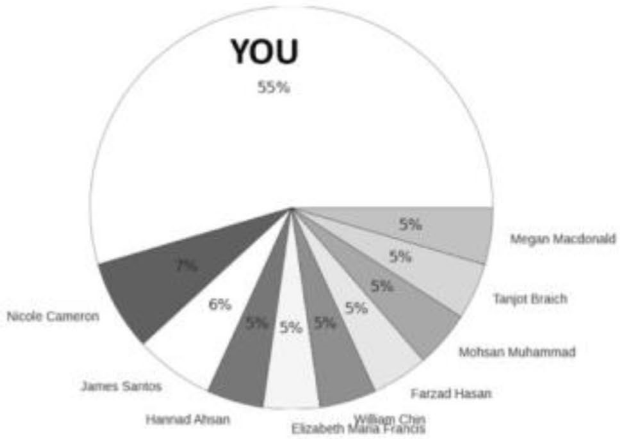
Imagine that an employer can view what you are saying on social media publicly

Posters

Example 1: Top 10 Contributors to a Group



Example 2: Top 10 Contributors to a Group



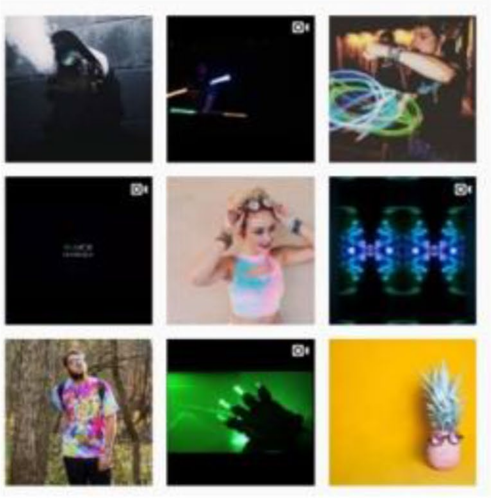
Imagine that an employer can view how active you are in a public online group

Table 10 (continued)

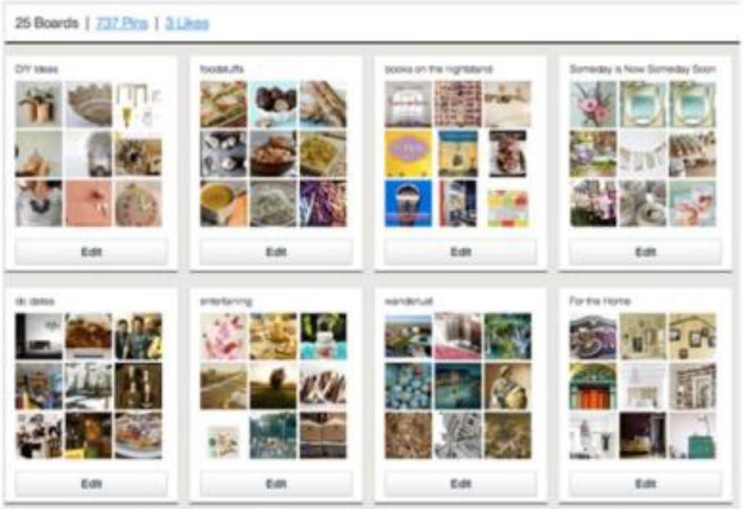
How comfortable would you be if an employer uses this information about you to make a hiring decision? [Likert scale 1–7; 1 = uncomfortable, 7 = comfortable]

Photos

Example 1: Your Shared Photos



Example 2: Your Shared Photos



25 Boards | 737 Pins | 3 Likes

Imagine that an employer can view photos that you shared on social media publicly

Appendix B: Measurement model for CFSMIP

Step 1: Principal component factor analysis

Based on the factor analysis, we discovered three factors related to privacy concerns: Collection, Errors, and a combined factor of Secondary Use and Unauthorized Access. UAC4 was excluded from the subsequent analysis as it loaded on more than one factor (Tables 11, 12, 13).

Table 11 KMO and Bartlett's Test

Kaiser–Meyer–Olkin measure of sampling adequacy	0.853
Bartlett's test of sphericity	
Approx. Chi-square	1966.204
df	91
Sig.	0.000

Table 13 Rotated component matrix

	Component		
	1	2	3
COL1	0.123	0.794	0.108
COL2	0.168	0.780	0.002
COL3	0.194	0.748	0.150
COL4	0.160	0.790	0.115
UAC1	0.648	0.076	0.203
UAC2	0.636	0.079	0.236
UAC3	0.706	0.011	0.113
UAC4	0.377	0.108	0.222
ERR1	0.056	0.167	0.786
ERR2	0.159	0.053	0.784
ERR3	0.196	0.077	0.801
SUS1	0.695	0.268	−0.027
SUS2	0.502	0.339	0.142
SUS3	0.694	0.264	−0.112

Extraction method: principal component analysis

Rotation method: varimax with Kaiser normalization

Rotation converged in 5 iterations

Table 12 Total variance explained

Component	Initial Eigenvalues			Rotation sums of squared loadings		
	Total	% of Variance	Cumulative %	Total	% of Variance	Cumulative %
1	4.444	31.740	31.740	2.854	20.388	20.388
2	1.760	12.572	44.312	2.739	19.563	39.951
3	1.502	10.730	55.042	2.113	15.091	55.042
4	0.916	6.543	61.585			
5	0.879	6.277	67.863			
6	0.650	4.644	72.506			
7	0.606	4.326	76.832			
8	0.573	4.091	80.923			
9	0.521	3.719	84.642			
10	0.472	3.372	88.014			
11	0.461	3.292	91.306			
12	0.434	3.101	94.408			
13	0.418	2.986	97.394			
14	0.365	2.606	100.000			

Extraction method: principal component analysis

Step 2: Reliability and discriminant validity checks

AVE for the combined variable of SUS & UAC is below the 0.5 threshold, thus it was removed from the subsequent analysis. The discriminant validity is within the accepted range for all variables (Tables 14, 15).

Table 14 Constructs' reliability and validity

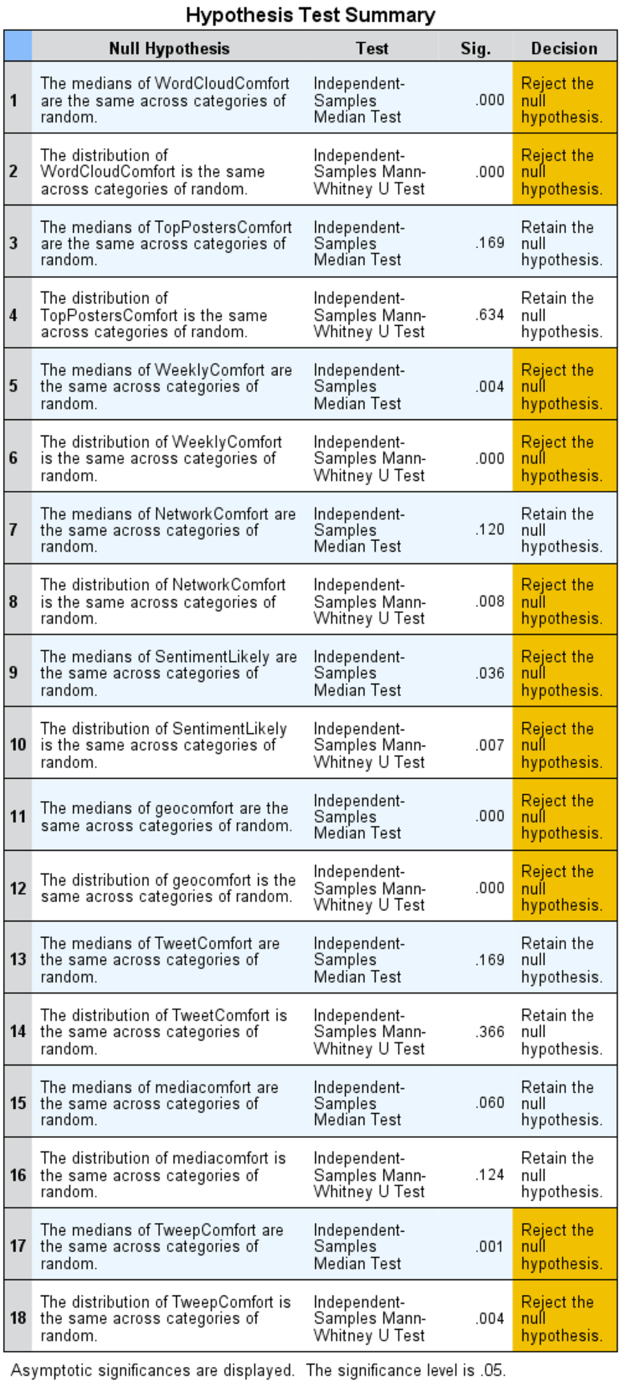
	Cronbach's Alpha	rho_A	Composite reliability	Average variance extracted (AVE)
Recommended threshold	≥ 0.7	≥ 0.7	≥ 0.7	≥ 0.5
COL	0.8217	0.8763	0.8773	0.642
ERR	0.7555	1.1651	0.833	0.6302
SUS & UAC	0.7706	0.7674	0.8033	0.4155

Table 15 Constructs' discriminant validity—HTMT

	COL	ERR
ERR	0.3172	
SUS & UAC	0.556	0.4287

Appendix C

Comparing the medians and distributions of the comfort scale questions between responses of Group A who saw visualization-based questions and Group B who only saw text-based questions.



Hypothesis Test Summary

	Null Hypothesis	Test	Sig.	Decision
1	The medians of WordCloudComfort are the same across categories of random.	Independent-Samples Median Test	.000	Reject the null hypothesis.
2	The distribution of WordCloudComfort is the same across categories of random.	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis.
3	The medians of TopPostersComfort are the same across categories of random.	Independent-Samples Median Test	.169	Retain the null hypothesis.
4	The distribution of TopPostersComfort is the same across categories of random.	Independent-Samples Mann-Whitney U Test	.634	Retain the null hypothesis.
5	The medians of WeeklyComfort are the same across categories of random.	Independent-Samples Median Test	.004	Reject the null hypothesis.
6	The distribution of WeeklyComfort is the same across categories of random.	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis.
7	The medians of NetworkComfort are the same across categories of random.	Independent-Samples Median Test	.120	Retain the null hypothesis.
8	The distribution of NetworkComfort is the same across categories of random.	Independent-Samples Mann-Whitney U Test	.008	Reject the null hypothesis.
9	The medians of SentimentLikely are the same across categories of random.	Independent-Samples Median Test	.036	Reject the null hypothesis.
10	The distribution of SentimentLikely is the same across categories of random.	Independent-Samples Mann-Whitney U Test	.007	Reject the null hypothesis.
11	The medians of geocomfort are the same across categories of random.	Independent-Samples Median Test	.000	Reject the null hypothesis.
12	The distribution of geocomfort is the same across categories of random.	Independent-Samples Mann-Whitney U Test	.000	Reject the null hypothesis.
13	The medians of TweetComfort are the same across categories of random.	Independent-Samples Median Test	.169	Retain the null hypothesis.
14	The distribution of TweetComfort is the same across categories of random.	Independent-Samples Mann-Whitney U Test	.366	Retain the null hypothesis.
15	The medians of mediacomfort are the same across categories of random.	Independent-Samples Median Test	.060	Retain the null hypothesis.
16	The distribution of mediacomfort is the same across categories of random.	Independent-Samples Mann-Whitney U Test	.124	Retain the null hypothesis.
17	The medians of TweepComfort are the same across categories of random.	Independent-Samples Median Test	.001	Reject the null hypothesis.
18	The distribution of TweepComfort is the same across categories of random.	Independent-Samples Mann-Whitney U Test	.004	Reject the null hypothesis.

Asymptotic significances are displayed. The significance level is .05.

References

Acquisti, A., & Grossklags, J. (2005). Privacy and rationality in individual decision making. *IEEE Security and Privacy, 3*, 26–33. https://doi.org/10.1109/MSP.2005.22.

Agerström, J., & Rooth, D.-O. (2011). The role of automatic obesity stereotypes in real hiring discrimination. *Journal of Applied Psychology, 96*, 790–805. https://doi.org/10.1037/a0021594.

Ajunwa, I., Crawford, K., & Schultz, J. (2017). Limitless worker surveillance. *California Law Review, 105*(3), 735–776. https://doi.org/10.15779/Z38BR8MF94.

Archer-Brown, C., Marder, B., Calvard, T., & Kowalski, T. (2018). Hybrid social media: Employees' use of a boundary-spanning technology. *New Technology, Work and Employment, 33*, 74–93. https://doi.org/10.1111/ntwe.12103.

Article 29 Data Protection Working Party. (2017). Opinion 2/2017 on data processing at work.

Bailey, J., & Steeves, V. (Eds.). (2015). *eGirls, eCitizens*. Ottawa, ON: University of Ottawa Press.

Bain, P., & Taylor, P. (2000). Entrapped by the 'electronic panopticon'? Worker resistance in the call centre. *New Technology, Work and Employment, 15*, 2–18. https://doi.org/10.1111/1468-005X.00061.

Ball, K. S., & Margulis, S. T. (2011). Electronic monitoring and surveillance in call centres: A framework for investigation: Surveillance in call centres. *New Technology, Work and Employment, 26*, 113–126. https://doi.org/10.1111/j.1468-005X.2011.00263.x.

Bazarova, N. N., & Choi, Y. H. (2014). Self-disclosure in social media: Extending the functional approach to disclosure motivations and characteristics on social network sites. *Journal of Communication, 64*, 635–657. https://doi.org/10.1111/jcom.12106.

Bergström, A. (2015). Online privacy concerns: A broad approach to understanding the concerns of different groups for different uses. *Computers in Human Behavior, 53*, 419–426. https://doi.org/10.1016/j.chb.2015.07.025.

Berkelaar, B. L. (2010). Cyber-vetting: Exploring the implications of online information for career capital and human capital decisions. PhD Dissertation. Purdue University, 3444477.

Berkelaar, B. L., & Harrison, M. A. (2017). Cybervetting. In C.R. Scott, L. Lewis (Eds.), *The international encyclopedia of organizational communication* (pp. 1–7). Hoboken: Wiley.

Berman, S. L., & Johnson-Cramer, M. E. (2016). Stakeholder theory: Seeing the field through the forest. *Business & Society, 58*, 1358–1375.

Bizer, C., Heese, R., Mochol, M., Oldakowski, R., Tolksdorf, R., & Eckstein, R. (2005). The impact of semantic web technologies on job recruitment processes. In O. K. Ferstl, E. J. Sinz, S. Eckert, & T. Isselhorst (Eds.), *Wirtschaftsinformatik 2005* (pp. 1367–1381). New York: Springer.

Boyd, D., & Crawford, K. (2012). Critical questions for big data. *Information, Communication & Society, 15*, 662–679.

CareerBuilder. (2014). Number of employers passing on applicants due to social media posts continues to rise, according to New CareerBuilder Survey - CareerBuilder [WWW Document]. Retrieved June 10, 2017, from https://www.careerbuilder.ca/share/aboutus/pressreleasesdetail.aspx?sd=6%2F26%2F2014&id=pr829&ed=12%2F31%2F2014.

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.

Chang, C.-W., & Heo, J. (2014). Visiting theories that predict college students' self-disclosure on Facebook. *Computers in Human Behavior, 30*, 79–86. https://doi.org/10.1016/j.chb.2013.07.059.

Chen, Z. T., & Cheung, M. (2018). Privacy perception and protection on Chinese social media: A case study of WeChat. *Ethics and Information Technology, 20*, 279–289. https://doi.org/10.1007/s10676-018-9480-6.

Chennamaneni, A., & Taneja, A. (2015). Communication privacy management and self-disclosure on social media—A case of Facebook. In AMCIS 2015 Proc.

Clark, L. A., & Roberts, S. J. (2010). Employer's use of social networking sites: A socially irresponsible practice. *Journal of Business Ethics, 95*, 507–525.

Clarkson, M. B. E. (1995). A stakeholder framework for analyzing and evaluating corporate social performance. *Academy of Management Review, 20*, 92–117. https://doi.org/10.2307/258888.

Couldry, N., & Powell, A. (2014). Big data from the bottom up. *Big Data & Society, 1*, 2053951714539277. https://doi.org/10.1177/2053951714539277.

Cranor, L. F., Reagle, J., & Ackerman, M. S. (1999). *Beyond concern: Understanding net users' attitudes about online privacy*. Florham Park: AT&T Labs-Research.

de Ville, V.-I. (2014). Young people as company stakeholders? Moving beyond CSR. *Young Consumers, 15*, 3–16. https://doi.org/10.1108/YC-03-2013-00363.

Debatin, B., Lovejoy, J. P., Horn, A.-K., & Hughes, B. N. (2009). Facebook and online privacy: Attitudes, behaviors, and unintended consequences. *Journal of Computer-Mediated Communication, 15*, 83–108. https://doi.org/10.1111/j.1083-6101.2009.01494.x.

Derous, E., Nguyen, H.-H., & Ryan, A. M. (2009). Hiring discrimination against Arab minorities: Interactions between prejudice and job characteristics. *Human Performance, 22*, 297–320.

Dinev, T., & Hart, P. (2006). An extended privacy calculus model for E-commerce transactions. *Information Systems Research, 17*, 61–80.

DiRomualdo, T., Girimonte, F., & Osle, H. (2018). The CHRO Agenda: Enabling enterprise digital transformation takes center stage. https://www.thehackettgroup.com/elq-key-issues-hr-1801/.

Donaldson, T., & Preston, L. E. (1995). The stakeholder theory of the corporation: Concepts, evidence, and implications. *Academy of Management Review, 20*, 65–91. https://doi.org/10.2307/258887.

Doolin, B., Dillon, S., Thompson, F., & Corner, J. L. (2005). Perceived risk, the Internet shopping experience and online purchasing behavior: A New Zealand perspective. *Journal of Global Information Management, 2*, 66–88.

Drake, J. R., Hall, D., Becton, J. B., & Posey, C. (2016). Job applicants' information privacy protection responses: Using social media for candidate screening. *AIS Transactions on Human Computer Interaction, 8*, 160–184.

Draper, N. A. (2016). From privacy pragmatist to privacy resigned: Challenging narratives of rational choice in digital privacy debates. *Policy Internet, 9*, 232–251. https://doi.org/10.1002/poi3.142.

Drennan, J., Mort, G. S., & Previte, J. (2006). Privacy, risk perception, and expert online behavior: An exploratory study of household end users. *Journal of Organizational and End User Computing, 18*, 1–22.

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.

Ellison, N. B., Steinfield, C., & Lampe, C. (2007). The benefits of Facebook "friends:" Social capital and college students' use of online social network sites. *Journal of Computer-Mediated Communication, 12*, 1143–1168. https://doi.org/10.1111/j.1083-6101.2007.00367.x.

Ellison, N. B., Steinfield, C., & Lampe, C. (2011). Connection strategies: Social capital implications of Facebook-enabled communication practices. *New Media & Society, 13*, 873–892. https://doi.org/10.1177/1461444810385389.

Finucane, M. L., Slovic, P., Mertz, C. K., Flynn, J., & Satterfield, T. A. (2000). Gender, race, and perceived risk: The "white male" effect. *Health, Risk & Society, 2*, 159–172. https://doi.org/10.1080/713670162.

Fogel, J., & Nehmad, E. (2009). Internet social network communities: Risk taking, trust, and privacy concerns. *Computers in Human Behavior, 25*, 153–160.

Forsythe, S. M., & Shi, B. (2003). Consumer patronage and risk perceptions in Internet shopping. *Journal of Business Research, 56*, 867–875. https://doi.org/10.1016/S0148-2963(01)00273-9.

Fortier, A., & Burkell, J. (2016). Display and control in online social spaces: Toward a Typology of users. *New Media & Society, 20*(3), 845–861.

Freeman, R. E. (1984). *Strategic management: A stakeholder approach*. Cambridge, UK: Cambridge University Press.

Freeman, R. E., Harrison, J. S., Wicks, A. C., Parmar, B. L., & Colle, S. (2010). *Stakeholder theory: The state of the art*. Cambridge: Cambridge University Press.

Frye, N. E., & Dornisch, M. M. (2010). When is trust not enough? The role of perceived privacy of communication tools in comfort with self-disclosure. *Computers in Human Behavior, 26*, 1120–1127. https://doi.org/10.1016/j.chb.2010.03.016.

Gandini, A., & Pais, I. (2017). Social recruiting: control and surveillance in a digitised job market. In P. V. Moore, M. Upchurch, & X. Whittaker (Eds.), *Humans and machines at work, dynamics of virtual work* (pp. 125–149). Cham: Palgrave Macmillan. https://doi.org/10.1007/978-3-319-58232-0_6.

Garbarino, E., & Strahilevitz, M. (2004). Gender differences in the perceived risk of buying online and the effects of receiving a site recommendation. *Journal of Business Research, 57*, 768–775. https://doi.org/10.1016/S0148-2963(02)00363-6.

Gibson, K. (2000). The moral basis of stakeholder theory. *Journal of Business Ethics, 26*, 245–257. https://doi.org/10.1023/A:1006110106408.

Goffman, E. (1959). *The presentation of self in everyday life*. Garden City, NY: Doubleday.

Gouvier, D. W., Jordan, S., & Mayville, S. (2003). Patterns of discrimination in hiring job applicants with disabilities: The role of disability type, job complexity, and public contact. *Rehabilitation Psychology, 48*, 175–181. https://doi.org/10.1037/0090-5550.48.3.175.

Greening, D. W., & Turban, D. B. (2000). Corporate social performance as a competitive advantage in attracting a quality workforce. *Business & Society, 39*, 254–280. https://doi.org/10.1177/000765030003900302.

Gruzd, A., Jacobson, J., & Dubois, E. (2017). You're hired: Examining acceptance of social media screening of job applicants. In *Proceedings of the 23rd Americas Conference on Information Systems*. Boston, MA. https://aisel.aisnet.org/amcis2017/DataScience/Presentations/28/.

Gruzd, A., Jacobson, J., Dubois, E., & Mai, P. (2018). *State of Social Media in Canada 2017*. Toronto: Ryerson University Social Media Lab. https://doi.org/10.5683/SP/AL8Z6R.

Gruzd, A., Jacobson, J., & Dubois, E. (in press). Cyber-vetting and the public life of social media data. *Social Media + Society*.

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 Information, 117*, 442–458. https://doi.org/10.1108/IMDS-04-2016-0130.

Hargittai, E. (2010). Digital na(t)ives? Variation in Internet skills and uses among members of the "net generation". *Sociological Inquiry, 80*, 92–113.

Hargittai, E., & Litt, E. (2013). New strategies for employment? Internet skills and online privacy practices during people's job search. *IEEE Security and Privacy, 11*, 38–45.

Hargittai, E., & Marwick, A. (2016). "What can I really do?" Explaining the privacy paradox with online apathy. *International Journal of Communication, 10*(21), 3737–3757.

Helm, P. (2018). Treating sensitive topics online: A privacy dilemma. *Ethics and Information Technology, 20*, 303–313. https://doi.org/10.1007/s10676-018-9482-4.

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

Horvath, M., & Ryan, A. M. (2003). Antecedents and potential moderators of the relationship between attitudes and hiring discrimination on the basis of sexual orientation. *Sex Roles, 48*, 115–130. https://doi.org/10.1023/A:1022499121222.

Howcroft, D., & Taylor, P. (2014). 'Plus ca change, plus la meme chose?'-researching and theorising the 'new' new technologies: Editorial. *New Technology, Work and Employment, 29*, 1–8. https://doi.org/10.1111/ntwe.12026.

Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising, 10*, 28–45.

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

Hurrell, S. A., Scholarios, D., & Richards, J. (2017). 'The kids are alert': Generation Y responses to employer use and monitoring of social networking sites. *New Technology, Work and Employment, 32*, 64–83.

Jacobson, J. & Gruzd, A. (2018). Employers' use of young people's social media: Extending stakeholder theory to social media data. In *Academy of Management Annual Meeting Proceedings*. Chicago, IL. https://doi.org/10.5465/AMBPP.2018.18217abstract.

Janta, H., & Ladkin, A. (2013). In search of employment: Online technologies and Polish migrants. *New Technology, Work and Employment, 28*, 241–253. https://doi.org/10.1111/ntwe.12018.

Jawahar, I. M., & McLaughlin, G. L. (2001). Toward a descriptive stakeholder theory: An organizational life cycle approach. *Academy of Management Review, 26*, 397–414.

Jeske, D., & Santuzzi, A. M. (2015). Monitoring what and how: psychological implications of electronic performance monitoring: Electronic performance monitoring of employees. *New Technology, Work and Employment, 30*, 62–78. https://doi.org/10.1111/ntwe.12039.

Jones, T. M., & Wicks, A. C. (1999). Convergent stakeholder theory. *Academy of Management Review, 24*, 206–221. https://doi.org/10.2307/259075.

Kennedy, H. (2016). *Post, mine, repeat*. London, UK: Palgrave Macmillan UK.

Krupa, T., Kirsh, B., Cockburn, L., & Gewurtz, R. (2009). Understanding the stigma of mental illness in employment. *Work, 33*, 413–425.

Leary, M. R., & Kowalski, R. M. (1990). Impression management: A literature review and two-component model. *Psychological Bulletin, 107*, 34–47.

Lin, J., Amini, S., Hong, J. I., Sadeh, N., Lindqvist, J., & Zhang, J. (2012). Expectation and purpose: Understanding users' mental models of mobile app privacy through crowdsourcing. In *Proceedings of the 2012 ACM Conference on Ubiquitous Computing*. ACM, pp. 501–510.

Lipford, H.R., Besmer, A., & Watson, J. (n.d.). Understanding Privacy Settings in Facebook with an Audience View. Usenix.

Litt, E. (2012). Knock, knock. Who's there? The imagined audience. *Journal of Broadcasting & Electronic Media, 56*, 330–345. https://doi.org/10.1080/08838151.2012.705195.

Livingstone, S. (2004). Media literacy and the challenge of new information and communication technologies. *The Communication Review, 7*, 3–14. https://doi.org/10.1080/10714420490280152.

Loh, W. (2018). A practice–theoretical account of privacy. *Ethics and Information Technology, 20*, 233–247. https://doi.org/10.1007/s10676-018-9469-1.

Lutz, C., & Strathoff, P. (2014). Privacy concerns and online behavior–Not so paradoxical after all? *Viewing the Privacy Paradox Through Different Theoretical Lenses*. https://doi.org/10.2139/ssrn.2425132.

Mai, J.-E. (2016). Big data privacy: The datafication of personal information. *The Information Society, 32*, 192–199. https://doi.org/10.1080/01972243.2016.1153010.

Mao, E., & Zhang, J. (2014). Gender differences in the effect of privacy on location-based services use on mobile phones. Presented at the Twentieth Americas Conference on Information Systems, Savannah, pp. 1–13.

Marwick, A., & Hargittai, E. (2018). Nothing to hide, nothing to lose? Incentives and disincentives to sharing information with institutions online. *Information, Communication & Society, 22*(12), 1697–1713. https://doi.org/10.1080/1369118X.2018.1450432.

Marwick, A. E., Murgia-Diaz, D., & Palfrey, J. G. (2010). *Youth, privacy and reputation (literature review) (SSRN Scholarly Paper No. ID 1588163)*. Rochester, NY: Social Science Research Network.

McEwan, B., & Flood, M. (2017). Passwords for jobs: Compression of identity in reaction to perceived organizational control via social media surveillance. *New Media & Society, 20*(5), 1715–1734.

Mellahi, K., Morrell, K., & Wood, G. (2010). *The ethical business: challenges and controversies*. London, UK: Palgrave Macmillan.

Nissenbaum, H. (2011). A contextual approach to privacy online. *Daedalus, 140*, 32–48.

O'Hara, B. (2004). Twice penalized: Employment discrimination against women with disabilities. *Journal of Disability Policy Studies, 15*, 27–34. https://doi.org/10.1177/10442073040150010501.

Okazaki, S., Li, H., & Hirose, M. (2009). Consumer privacy concerns and preference for degree of regulatory control. *Journal of Advertising Research, 38*, 63–77. https://doi.org/10.2753/JOA0091-3367380405.

Osatuyi, B. (2015). Empirical examination of information privacy concerns instrument in the social media context. *AIS Transactions on Replication Research, 1*, 1–14.

Oshima, T., & Dell-Ross, T. (2016). All possible regressions using IBM SPSS: A practitioner's guide to automatic linear modeling. In: Georgia Educational Research Association Conference.

Palfrey, J., & Gasser, U. (2010). *Born digital: Understanding the first generation of digital natives*. New York: Basic Books.

Pedersen, S., Burnett, S., Smith, R., & Grinnall, A. (2014). The impact of the cessation of blogs within the UK police blogosphere: Impact of the cessation of blogs. *New Technology, Work and Employment, 29*, 160–176. https://doi.org/10.1111/ntwe.12028.

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

Petit, P. (2007). The effects of age and family constraints on gender hiring discrimination: A field experiment in the French financial sector. *Labour Economics, 14*, 371–391. https://doi.org/10.1016/j.labeco.2006.01.006.

Quan-Haase, A., & Young, A. L. (2010). Uses and gratifications of social media: A comparison of Facebook and instant messaging. *Bulletin of Science, Technology & Society, 30*, 350–361. https://doi.org/10.1177/0270467610380009.

Regan, P. M., & Jesse, J. (2018). Ethical challenges of edtech, big data and personalized learning: Twenty-first century student sorting and tracking. *Ethics and Information Technology, 21*(3), 167–179. https://doi.org/10.1007/s10676-018-9492-2.

Richey, M., Gonibeed, A., & Ravishankar, M. N. (2017). The perils and promises of self-disclosure on social media. *Information Systems Frontiers, 20*(3), 425–437. https://doi.org/10.1007/s10796-017-9806-7.

RiskAware [WWW Document]. (2017). Retrieved June 10, from, 2017 https://riskaware.com/our-products/social-media-screening/.

Rosenberg, M., & Dance, G. J. X. (2018). *'You are the product': Targeted by Cambridge Analytica on Facebook*. New York: New York Times.

Schrodt, P. (2013). Content relevance and students' comfort with disclosure as moderators of instructor disclosures and credibility in the college classroom. *Communication Education, 62*, 352–375. https://doi.org/10.1080/03634523.2013.807348.

Sheehan, K. B. (2002). Toward a typology of Internet users and online privacy concerns. *The Information Society, 18*, 21–32.

Shen, G., Jia, J., Nie, L., Feng, F., Zhang, C., & Hu, T. (2017). Depression detection via harvesting social media: A multimodal dictionary learning solution. In Proceedings of the Twenty-Sixth International Joint Conference on Artificial Intelligence (IJCAI-17) pp. 3838–3844.

Smith, A. (2015). *Searching for work in a digital era*. Washington: Pew Research Center.

Spake, D. F., Beatty, S. E., Brockman, B. K., & Crutchfield, T. N. (2003). Consumer comfort in service relationships: Measurement and importance. *Journal of Service Research, 5*, 316–332.

Spake, D. F., Zachary Finney, R., & Joseph, M. (2011). Experience, comfort, and privacy concerns: Antecedents of online spending. *Journal of Research in Interactive Marketing, 5*, 5–28. https://doi.org/10.1108/17505931111121507.

Stark, L. (2016). The emotional context of information privacy. *The Information Society, 32*, 14–27. https://doi.org/10.1080/01972243.2015.1107167.

Statistica. (2017a). Facebook users worldwide 2017 [WWW Document]. Statista. Retrieved November 11, 2017, from https://www.statista.com/statistics/264810/number-of-monthly-active-facebook-users-worldwide/.

Statistica. (2017b). Instagram - Statistics & Facts [WWW Document]. www.statista.com. Retrieved November 11, 2017, from https://www.statista.com/topics/1882/instagram/.

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

Stone, D. L., & Stone-Romero, E. F. (1998). A multiple stakeholder model of privacy in organizations. In M. Schminke (Ed.), *Managerial Ethics: Moral management of people and processes* (pp. 35–60). Mahwah, N.J.: Psychology Press.

Suh, J. J., & Hargittai, E. (2015). Privacy management on Facebook: Do device type and location of posting matter? *Social Media Society, 1*, 1–11.

Townsend, L., & Wallace, C. (n.d.). Social media research: A guide to ethics (No. Economic and Social Research Council [Grant Number ES/M001628/1]). University of Aberdeen.

Tsai, W.-C., & Yang, I. W.-F. (2010). Does image matter to different job applicants? The influences of corporate image and applicant individual differences on organizational attractiveness. *International Journal of Selection and Assessment, 18*, 48–63.

Turban, D. B., & Greening, D. W. (1997). Corporate social performance and organizational attractiveness to prospective employees. *Academy of Management Journal, 40*, 658–672. https://doi.org/10.2307/257057.

Tverdek, E. (2008). What makes information “public”? *Public Affairs Quarterly, 22*, 63–77.

Visser, W., Matten, D., Pohl, M., & Tolhurst, N. (2010). *The A to Z of corporate social responsibility*. West Sussex, UK: Wiley.

Weber, J. (2017). Understanding the millennials’ integrated ethical decision-making process: Assessing the relationship between personal values and cognitive moral reasoning. *Business & Society, 58*(8), 1671–1706.

Westin, A. F. (2000). Intrusions. *Public Perspective*, *11*(6), 8–11.

Whiting, A., & Williams, D. (2013). Why people use social media: A uses and gratifications approach. *Qualitative Market Research: An International Journal, 16*, 362–369. https://doi.org/10.1108/QMR-06-2013-0041.

Williams, D. L., Crittenden, V. L., Keo, T., & McCarty, P. (2012). The use of social media: An exploratory study of usage among digital natives. *Journal of Public Affairs, 12*, 127–136. https://doi.org/10.1002/pa.1414.

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

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

Publisher’s Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.