The Unethical Side of Cybervetting

Kara Estes

Bellevue University

MBPC 680: Business and Professional Communications Capstone

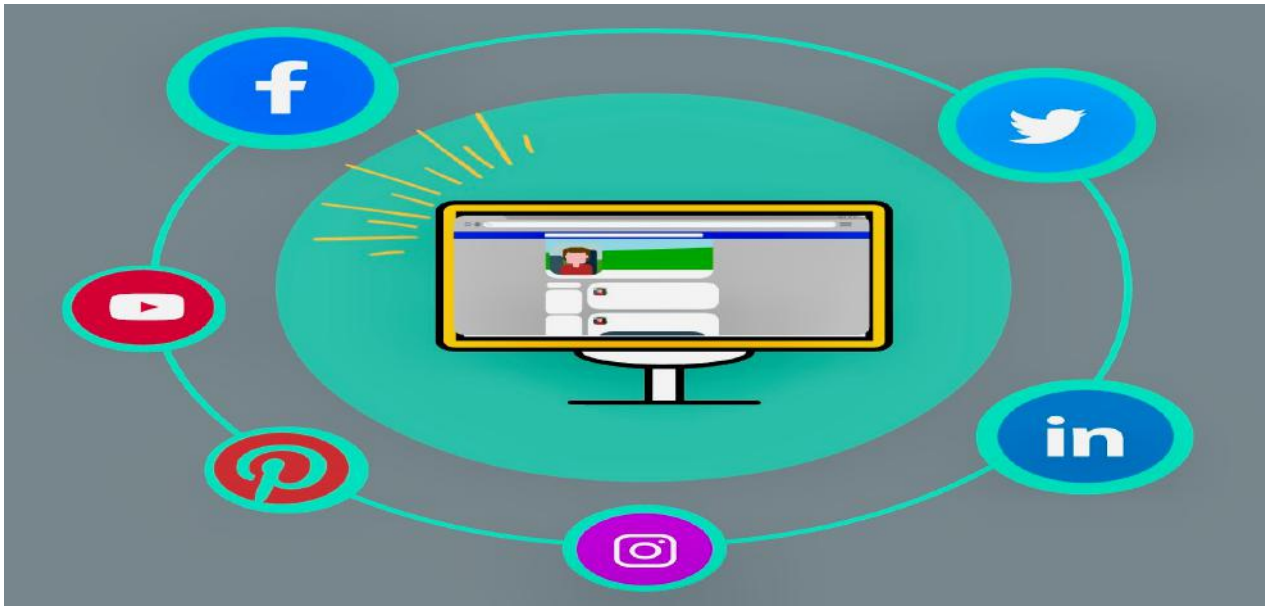
Dr. Kate Joeckel

February 21, 2021

EXECUTIVE SUMMARY

How ethical is it for a company to conduct a cybervetting search on an applicant without the applicant's permission? Cybervetting is when employers use the internet or a social media search to gain information about applicants to make informed employment decisions. Cybervetting is cheap and an easy way to determine who an applicant truly is outside of their resume. Cybervetting can give an employer a snapshot of the applicant, all without the applicant ever knowing. The social media snapshot can tell an employer all about the applicant. The employer can determine if the applicant drinks or does illicit drugs, posts salacious pictures, talks poorly about an employer, and or even their writing skills. The downfall of cybervetting is that it does not account for when the applicant has an internet personality that differs from their actual persona or post for show and not the truth.

Cybervetting does not give the outside reader any context to the post, which could be vital to understanding. Employers may not always understand the post's context or follow the same online social circles as the applicant. While there is no law to prevent a company from conducting cybervetting, some state laws are in place to help protect the applicant. Ethically if a company performs cybervetting, they are at risk of violating an applicant's privacy. A person can learn protected information once they view an applicant's profile, leaving them open to a possible discrimination complaint. Cybervetting is not new, causing applicants to become more aware of their presence while hunting for a job. Even though applicants have become more concerned about their privacy and are using privacy settings to protect their opinions, employers question what the applicant might be hiding. While the law is starting to catch up in various states, cybervetting usage becomes more questionable and unethical in today's social media filled world.



INTRODUCTION

Social media (SM) has become a vital part of our daily lives. As of 2020, global internet users spent over two hours a day browsing and posting to SM sites like Facebook, Instagram, Twitter, and various others (Henderson, 2020). Over 9000 tweets are sent every second containing a moment in the users' lives, likes, thoughts, emotions, and ideals (Bagadiya, 2021). We now live our lives not online in the real world but also in the cyberworld through SM. We pick and choose what image of ourselves we present for the world to see. We have shifted our lives from being personal to digital, sharing our moments with anyone in the world who wants to read about us. With the shift towards digital, employers have discovered that SM is a goldmine of information and can be explicitly used to conduct background checks on prospective employees called cybervetting. Cybervetting is when a company uses information found online to research a person for a job, university admissions, even for dating (Jeske & Shultz, 2015). SM was created as a tool used to share our lives with friends and family but has turned into a tool to judge a person's character (Rosen et al., 2018). A hiring manager can find out considerable information about a person by just searching their SM posts. A simple search can help a person find out what another's hobbies are, past times, what they look like, their religion, medical conditions, education, and other various data.

With all the status updates we post on SM, one would think an HR manager would not want to know what kind of cake an applicant ate for their birthday, but employers beg to differ. Any information they can find can tell them more about who the applicant is and what kind of worker they will be, how they handle pressure; they can even find the applicant's cake flavor preference. Full background checks are expensive, while conducting cybervetting is cheap, if not free (Albert et al., 2019). Using a search engine, a company can likely uncover most of the same information a background check will provide, along with so much more such as drug and alcohol usage, homophobic or racist remarks, communication skills, and speaking poorly of a former

employer. Job applicants are finding that since employers use cybervetting, they see fewer job offers for jobs they were genially qualified for due to what they post on SM (Alexander et al., 2019). A picture or status update may have seemed fun and harmless when the applicant posted it, but down the road, it could be the reason why they did not get a job (Dayton Daily News, 2017).

There are no laws to prevent an employer from reviewing an applicant's SM posts (Maurer, 2018). Employers are not required to get a signature from the applicant before conducting a cybervetting search (Albert et al., 2019). Applicants can utilize privacy settings on their SM profiles to prevent unwanted eyes from seeing their posts (Gruzd et al., 2020). Privacy settings allow a user to decide who can see their SM posts. Most SM sites allow users to set either a default privacy setting or pick and choose which posts can be public or private. However, the use of privacy settings can cause an employer to wonder what the applicant is hiding (Dayton Daily News, 2017)—leaving an applicant to choose if they value their privacy or a future job the most (Haller & Ball, 2020). Employers hold all the power when they decide to hire based on an online presence or lack of presence (Gruzd & Dubois, 2020). Cybervetting is only a benefit for the employer, leaving applicants at a disadvantage for sharing their life with the people they chose to share. Ethically, should a prospective employer hold this much power over an applicant based on their personal life, and at what point does it not become a violation of privacy? This white paper will be reviewing how cybervetting is unethical when it violates an applicant's privacy, specifically the ethics of judging an applicant with information that was not created for them to see.

BACKGROUND

(Benitez, 2016)

Cybervetting is when employers acquire information about applicants from informal, non-institutional, online sources such as SM profiles to make informed employment decisions (Berkelaar & Harrison, 2016). Cybervetting uses unconventional sources such as Facebook, Twitter, Instagram, LinkedIn, YouTube, Reddit, Tumblr, or blogs to conduct a background check (Jeske & Shultz, 2015). When companies view an applicant's SM posts, they look at everything from the posts' content to posts' frequency of posts (Becton et al., 2019). Employers expect to see an applicant's robust SM profile with an active presence on the service showcasing a brand that would benefit the company (Dayton Daily News, 2017). Companies do not want to see an applicant negative posting about drinking, doing drugs, illegal activities, poor

communication skills, or bad-mouthing an employer (Becton et al., 2019). Cybervetting stifles prospective employees from speaking openly about having a drink with friends or prevents them from using informal internet shorthand when posting on SM for fear of missing a job opportunity. Employers could find themselves passing on a highly qualified applicant because of a post from a bad day at work. Cybervetting has blurred the line regarding what a person can post on SM to reflect their values versus the prospective company or employer's values.

Creative HR Managers

Businesses want higher profits with lower operating costs, which have led HR managers to become creative when vetting an applicant at the cost of smaller budgets (Jacobson & Gruzd, 2020). Cybervetting only costs time, effort, and internet access to complete. All a person must do is Google the applicant's name or search by their email address or phone number on SM platforms to conduct their background check (Klimas, 2010). Most HR managers think they can get a good look into an individual's personality by cybervetting (Reda, 2019). SM presents the reader with the user's unfiltered thoughts (Rosen et al., 2018), a snapshot of a person, and a moment of their life (Blount et al., 2016), the most accurate version of the applicant (Rosen et al., 2018).

Employers want an applicant that is a good fit with the company, and by searching SM posts, employers think they will find the best person for the job. A recent study found that 70% of employers use social network sites to research an applicant, while seven percent plan to start. Of those who do research, 57% have found content that caused them not to hire an applicant (CareerBuilder, 2018). Companies fear that applicants are dishonest with them during the hiring process. Hiring managers have taken to heart the ideals that everyone lies, and the only time a person appears to be perfect is during a job interview. A bad hire could cost the company anywhere from 25% to 500% of that person's salary based on the costs to find a replacement, training, and productivity loss (Pike et al., 2017). One way to uncover this dishonesty is the use of cybervetting as a tool to expose falsehoods that a candidate might try to pass using their resume or during their interview (Berkelaar & Buzzanell, 2014). Unlike background checks that require permission to run, candidates will never know if an employer reviewed their SM posts. A qualified candidate may never know they were passed over for a job because of an SM post the employer found, regardless of whether it is the correct person (Klimas, 2010).

THE PROBLEM: PEOPLE LIVE ONLINE

The separation between private and work life is becoming blurrier with social media as more employers are using it to research candidates (Lam, 2016). While the internet allows for some anonymity level over what people choose to share (Davison et al., 2011), people still tend to overshare intimate details about their lives, including where they work, what position they hold, their family, even where they live. Over 87% of American's tend to spend at least an hour a day, if not more, browsing and posting to SM (Lam, 2016). People tend to create identities for whom they want to be when they are online. People pick and choose what they want others to perceive

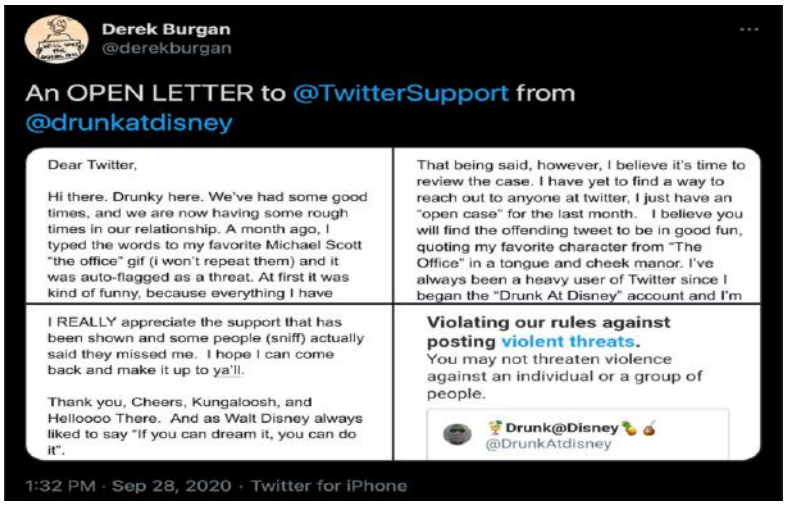
them to be (Rosen et al., 2018), which might not be the best reflection of who they are in real life (Hazelton & Terhorst, 2015). A candidate can seem to be an outgoing influencer in an SM circle with many followers when they are quiet, shy, and less outgoing. The outgoing internet persona and the reserved in-person persona are the same people; they just present different parts of their identity when it is relevant (LaCour, 2014)—thus making cybervetting results potentially inaccurate when an online personality differs from an in-person persona.

Online persona vs in person persona

To determine the most accurate persona of a candidate, companies use LinkedIn as a business personality source. LinkedIn allows candidates to present an SM version of a resume as their profile. Users tend to post a more professional version of themselves, letting users see a glimpse of their professionalism. However, with any SM site, information put on LinkedIn is there to make the user look good, regardless of the truthfulness (Melão & Reis, 2020).
When companies use cybervetting and search multiple SM sites, they might get a different impression of a candidate depending on which SM site they use. Leaving the question of is it ethical to judge a person's best fit based on incomplete information, out-of-context posts, or multiple personas (Rosen et al., 2018)? Companies should also take into consideration if they found the correct person's profile. Many people share the same name, which could cause an HR Manager to conclude using wrong information about an otherwise viable applicant (De Armond, 2017). Ethically, companies who conduct cybervetting should have safeguards in place to verify the profile and persona used (Hazelton & Terhorst, 2015), giving candidates a chance to confirm, answer and or justify their online persona or posts.

Contextual mistakes

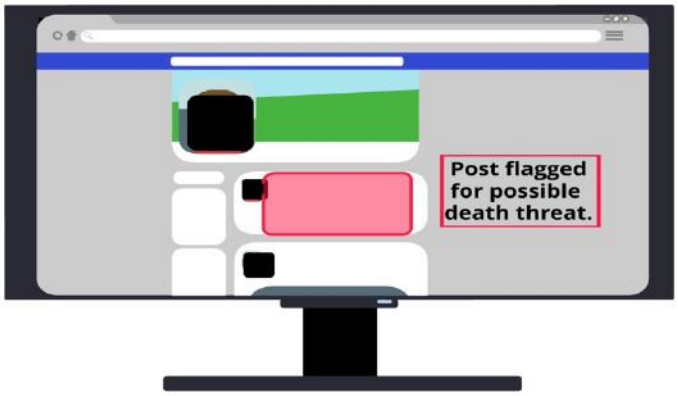
When a candidate posts on SM, they are likely to cater to their friends, family, or like-minded individuals (CareerBuilder, 2018). Applicants contextualize their SM updates toward an SM inner circle, filled with people who will understand the context (Pike et al., 2017). A popular Twitter account, @DrunkAtDisney, sent a tweet to a parody Twitter account for a fake liver called @RhiannonsLiver. The tweet referenced a quote meme of Michael Scott from The Office saying, "I'm going to kill you (Burgan, 2020)." The tweet's context was humorous and taken in good spirits, a joke to those in the same SM circle. However, an outsider, such as a hiring manager, might not understand the post's comical context, thus deeming the tweet harmful, resulting in a failed cybervetting result (Pike et al., 2017).



(Burgan, 2020)

Applicant's background

Before hiring, most companies conduct a background check of an applicant. The background check serves to research prior job history, criminal convictions, and credit ratings (Hazelton & Terhorst, 2015). When a company does a background check, they are required by the law of the Fair Credit Reporting Act (FCRA) to get a signature from the applicant, therefore notifying them and obtaining their authorization for the review (Albert et al., 2019). With cybervetting, there are no notification requirements nor a need for a signature from the applicant to conduct the review (Maurer, 2018). Some companies are now using a third-party service for cybervetting, which gives them a pass or fail grade for the applicant based on what was found during their search (Reicher, 2013). These companies use the FCRA as guidance for reviewing SM posts, only using verified information and posts for up to seven years (Maurer, 2018). These th10ird-party companies allow a business to hire them and get a report that leaves out any EEOC-protected information in the results, giving screenshot examples of posts and why they were flagged. Applicants must sign a waiver for the third parties to conduct their search, and their reports are updated as information and the addition or deletion of a post changes. All pictures in the report are cropped out to prevent any disclosure of protected classes, with the report allowing for the applicant to dispute any information found (Browning, 2012). The reports give a company a pass or fail grade, letting the company make the final decision based on non-discriminatory information (Reicher, 2013). Getting permission, albeit through a third-party company or by having the applicant consent to cybervetting, would be the best way if a company is determined to conduct any cybervetting check. Third-party companies make the process less of a violation of privacy, with a report that allows users to dispute any information while keeping a company secure from a possible EEOC complaint.



(Hill, 2011)

THE PROBLEM: PRIVACY

SM is typically considered an open platform. Typically, when users post without privacy settings engaged, the post defaults to public viewing, allowing anyone with access to the site to view, like, or share (Jacobson & Gruzd, 2020). With SM considered an open platform, users have no privacy expectation, even when users post gearing towards specific individuals (Hosain & Liu, 2019). Meaning once it is out there for the world to see, it is fair game for anyone to see and use. SM is permanent; even when a post is deleted, there is a possibility of someone screenshot it and can post it elsewhere for others to find (Alexander et al., 2019). Most SM platform's privacy setting default to the public when a user creates their profile. It is up to the user to determine

what is shared publicly versus privately. While an applicant can change their privacy settings to prevent unwanted eyes from seeing their posts, it does not prevent an employer from requesting privacy settings be changed or asking to see what is being posted (Delarosa, 2016). While privacy may allow the user to feel secure in what they say online, it does not mean employers will not be questioning what they are hiding (Cook et al., 2020).

The law and cybervetting

As of 2021, there is no Federal law in the United States that prohibits an employer from conducting cybervetting (Maurer, 2018). Without any required disclosures, most applicants will never know their SM posts were examined. On the local level, 26 states have passed laws regarding applicants, employees, and students' online privacy to prevent employers and universities from requesting passwords to personal Internet accounts to get or keep a job (Greenberg, 2020). The state laws act as more of a superhero identity protection law; they prevent employees or applicants from revealing or giving their username, password, or become friends/followers of an employer university. The laws protect applicants from revealing their online identities (Workplace Fairness, 2020); however, no law currently protects applicants or employees from an employer conducting cybervetting or monitoring their SM.

Bias after searching

One of the best parts of SM is that it showcases a person. When a company reviews a candidate's SM profile, they can gain protected information about the person (Jeske & Shultz, 2015). A searcher can see pictures of the person, their family, medical history, and even disabilities (Sameen & Cornelius, 2013). The Equal Employment Opportunity Commission protects against age, disability, race/color, pregnancy, and religion, all of which an employer can gain by reviewing an SM profile (EEOC, 2020).

When a company starts receiving applications, they can start conducting a pass over the person's SM account, cybervetting them before an interview, and the first step in learning who the individual is personally (Jacobson & Gruzd, 2020). Learning this information can result in biases or discrimination (Melão & Reis, 2020). Once a company views the person's SM account, it is like opening the Equal Employment Opportunity Commission (EEOC) version of a Pandora's Box; there is no going back from knowing the information gained by reviewing an applicant's profile (Albert et al., 2019). If an applicant is not hired and should file a discrimination claim, the company will find it difficult to defend against the knowledge they gained when reviewing the applicant's SM (Klimas, 2010).

Discrimination based on a profile

Cybervetting can lead to new forms of discrimination not covered under the EEOC. Discrimination can happen because the applicant has a private profile, lack of social media influence, lack of followers or friends, or even if they use a photo filter that can predict the applicant's mental health of the applicant (Jacobson & Gruzd, 2020). Applicants can also endure

demographic biases. While the internet seems to be readily available, there is still a disparity between the internet's affordability, leaving lower-income or rural individuals disadvantaged (Sameen & Cornelius, 2013). When applicants lack internet access, they are likely not to have an SM profile, leaving employers thinking they are incompetent (Cook et al., 2020). Age discrimination is also a concern when it comes to cybervetting. Younger generations grew up with SM and tended to share a lot about their lives on different platforms (Albert et al., 2019). Older generations are the opposite and tend to shy away from having a robust SM platform (Yeung, 2019). A company could pass on an applicant for having too many or not enough SM posts, creating a bias when hiring (Albert et al., 2019).

THE SOLUTION

Applicants have a right to privacy, just like employers have a right to protect their brand (Gruzd & Dubois, 2020). Companies need to be more transparent about their cybervetting policies, urging for written permission from applicants to review their social media posts and having open dialogue when questionable material is discovered (Hosain & Liu, 2019). Lack of transparency can cause a company's brand to suffer from a lack of trust (Albert et al., 2019). When applicants lack confidence in a company because of its cybervetting techniques, the company loses out on the potential to recruit highly qualified applicants (Hosain & Liu, 2019). (Albert et al., 2019). Employers should be more open about cybervetting; being more upfront and transparent can lead to more trust from applicants.

Applicants strike back

Applicants have caught up with cybervetting tactics and are working to prevent their privacy from being invaded while maintaining a professional image. Even if companies are not transparent regarding their cybervetting techniques, applicants are protecting themselves. While many people know that one can learn a lot about an individual based on what they post, they agree that a person's privacy must be violated to learn this information. Violation of privacy does not sit well with most people (Cook et al., 2020). While most companies do not advertise their cybervetting techniques, applicants have solved this issue on their own. When people know they are being watched, they are likely to clean up their profiles and only present a positive professional image (Gruzd et al., 2020).

Applicants feel more pressure to conform to what an employer is looking for and less likely to give any other impression than a perfect worker (Jeske & Shultz, 2015). Therefore, the image that an employer gets is not the correct image of the actual applicant. A recent trend has seen applicants go to a more private privacy setting when searching for a job as a way of protecting their privacy, along with keeping prospective employers from finding out about their online persona and daily life online (Haller & Ball, 2020).

CONCLUSION

The first version of SM was invented in 1997 (Samur, 2018). Cybervetting began to gain popularity six years later with the rise of MySpace (Delarosa, 2016), disregarding the questions of its ethical use. Nothing has changed since cybervetting became popular. Applicants and HR managers are still asking the same moral question as they did in 2007 (Davison et al., 2011). Without any future laws or regulations, applicants and HR managers will likely be facing the same ethical questions and violations ten years from now (Haller & Ball, 2020). Companies should be cautious when using cybervetting (Jeske & Shultz, 2015). While they may be looking for the best fit ethically, they are also putting themselves and the company at risk for possible discrimination lawsuits and losing brand trust (Albert et al., 2019). While companies may feel they are using cybervetting to find the best candidate, they could be losing their credibility for not disclosing their cybervetting practice. Cybervetting could cause a company to pass on potentially highly qualified candidates who decided to live their life on SM (Gruzd & Dubois, 2020).

While cybervetting is not new, currently, there are not enough studies to validate the benefits of cybervetting to get a good fit versus the risk of bias hiring (Jeske & Shultz, 2015). Ethically, companies should be more transparent about their SM vetting practices, giving an applicant a chance to verify, dispute, or provide the context of their SM posts. Without transparency, cybervetting remains unethical, with companies are running the risk of bias hiring decisions, discrimination complaints, and damaging their brand. With applicants becoming more aware of the company's unethical cybervetting tactics, they will go to new ways of protecting their privacy, nulling any information gained from cybervetting. Until there are federal laws regarding cybervetting practices, ethically, companies should protect themselves and shy away from the practice to avoid possible lawsuits or brand-damaging claims.

References

Albert, L. J., Da Silva, N., & Aggarwal, N. (2019). Demographic differences and HR professionals' concerns over the use of social media in hiring. *e - Journal of Social & Behavioural Research in Business*, *10*(1), 1–9. https://www-proquest-com.ezproxy.bellevue.edu/scholarly-journals/demographic-differences-hr-professionals-concerns/docview/2260995521/se-2?accountid=28125

Alexander, E. C., Mader, D. D., & Mader, F. H. (2019). Using social media during the hiring process: A comparison between recruiters and job seekers. *Journal of Global Scholars of Marketing Science*, *29*(1), 78–87. https://doi.org/10.1080/21639159.2018.1552530

Bagadiya, J. (2021, January 13). *367 social media statistics you must know in 2021*. Social Pilot. https://www.socialpilot.co/blog/social-media-statistics

Becton, J. B., Walker, H. J., Gilstrap, J., & Schwager, P. H. (2019). Social media snooping on job applicants. *Personnel Review*, *48*(5), 1261–1280. https://doi.org/10.1108/pr-09-2017-0278

Benitez, G. A. (2016, October 3). *Cybervetting: How private is your digital information?* Penn State. https://sites.psu.edu/scarlethartigablog/2016/10/03/cyber-vetting/

Berkelaar, B. L., & Buzzanell, P. M. (2014). Cybervetting, person–environment fit, and personnel selection: Employers' surveillance and sensemaking of job applicants' online information. *Journal of Applied Communication Research*, *42*(4), 456–476. https://doi.org/10.1080/00909882.2014.954595

Blount, J., Wright, C. S., Hall, A. A., & Bliss, J. L. (2016). *Social media: Creating student awareness of its use in the hiring process* [PDF]. SFA ScholarWorks. https://scholarworks.sfasu.edu/businesscom_facultypubs/57/

Browning, J. (2012). *Why HR Managers are reading your Facebook page*. D Magazine. https://www.dmagazine.com/publications/d-ceo/2012/january-february/why-recruiters-use-social-media-background-checks/

Burgan, D. [@derekburgan]. (2020, September 28). *An open letter to @TwitterSupport from @drunkatdisney* [Tweet with a letter to Twitter] [Tweet]. Twitter. https://twitter.com/derekburgan/status/1310648512552599552?s=20

CareerBuilder. (2018, August 9). *More than half of employers have found content on social media that caused them not to hire a candidate, according to a recent Careerbuilder survey*. Press Room | Career Builder. Retrieved January 13, 2021, from 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

Cook, R., Jones-Chick, R., Roulin, N., & O'Rourke, K. (2020). Job seekers' attitudes toward cybervetting: Scale development, validation, and platform comparison. *International Journal of Selection and Assessment*, *28*(4), 383–398. https://doi.org/10.1111/ijsa.12300

Davison, H., Maraist, C., & Bing, M. N. (2011). Friend or foe? The promise and pitfalls of using social networking sites for HR decisions. *Journal of Business and Psychology*, *26*(2), 153–159. https://doi.org/10.1007/s10869-011-9215-8

Dayton Daily News. (2017, July 14). *What is cyber-vetting? It could cost you your job*. https://www.daytondailynews.com/business/what-cyber-vetting-could-cost-you-your-job/WIkQ36TercnDFlIGQH3UEI/

De Armond, M. (2017, September 1). *The Pros and Cons of Using Social Media in Vetting Job Applicants*. HigherEdJobs. https://www.higheredjobs.com/Articles/articleDisplay.cfm?ID=1394

Delarosa, J. (2016). From due diligence to discrimination: employer use of social media vetting in the hiring process and potential liabilities. *Loyola of Los Angeles Entertainment Law Review*, *35*(3), 249–280.

EEOC. (2020). *Employees and job applicants*. U.S. equal employment opportunity commission. Retrieved December 16, 2020, from https://www.eeoc.gov/employees-job-applicants

Greenberg, P. (2020, July 20). *State social media privacy laws*. NCSL: National Conference of State Legislatures. Retrieved February 1, 2021, from https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-prohibiting-access-to-social-media-usernames-and-passwords.aspx

Gruzd, A., & Dubois, E. (2020, July 8). *Companies are increasingly turning to social media to screen potential employees*. The Conversation. https://theconversation.com/companies-are-increasingly-turning-to-social-media-to-screen-potential-employees-141926

Gruzd, A., Jacobson, J., & Dubois, E. (2020). Cybervetting and the public life of social media data. *Social Media + Society*, *6*(2), 205630512091561. https://doi.org/10.1177/2056305120915618

Haller, B., & Ball, D. R. (2020). The legal and ethical considerations of using social media in the recruiting and hiring stages of employment. *Faculty Works: Business*, *82*, 452–560. https://digitalcommons.molloy.edu/bus_fac/82

Hazelton, A. S., & Terhorst, A. (2015). *Legal and ethical considerations for social media hiring practices in the workplace*. ScholarWorks at WMU. https://scholarworks.wmich.edu/hilltopreview/vol7/iss2/7/

Henderson, G. (2020, August 24). *How much time does the average person spend on social media?* https://www.digitalmarketing.org/blog/how-much-time-does-the-average-person-spend-on-social-media

Hill, K. (2011, June 15). *Feds okay start-up that monitors employees' internet and social media footprints*. Forbes. https://www.forbes.com/sites/kashmirhill/2011/06/15/start-up-that-monitors-employees-internet-and-social-media-footprints-gets-gov-approval/?sh=1d367c4f6411

Hosain, S., & Liu, P. (2019). Conducting pre-employment background checks through social networking sites: The new role of HR professionals. *Bizinfo Place*, *10*(2), 111–123. https://doi.org/10.5937/bizinfo1902111s

Jacobson, J., & Gruzd, A. (2020). Cybervetting job applicants on social media: The new normal? *Ethics and Information Technology*, *22*(2), 175–195. https://doi.org/10.1007/s10676-020-09526-2

Jeske, D., & Shultz, K. S. (2015). Using social media content for screening in recruitment and selection: Pros and cons. *Work, Employment and Society*, *30*(3), 535–546. https://doi.org/10.1177/0950017015613746

Klimas, K. (2010, June 19). *Should social media be used as a recruiting and screening tool?* Clarifacts. https://clarifacts.com/industry-insights/social-media-and-recruiting/

LaCour, K. (2014, November 6). *The online identity crisis*. WIRED. https://www.wired.com/insights/2014/11/the-online-identity-crisis/

Lam, H. (2016). Social media dilemmas in the employment context. *Employee Relations*, *38*(3), 420–437. https://doi.org/10.1108/er-04-2015-0072

Maurer, R. (2018, April 23). *Screening candidates' social media may lead to TMI, discrimination claims*. SHRM. Retrieved December 12, 2020, from https://shrm.org/resourcesandtools/hr-topics/talent-acquisition/pages/screening-social-media-discrimination-claims.aspx?_ga=2.223997019.1727199582.1607794276-7933865.1606881492

Melão, N., & Reis, J. (2020, June 24). *Using social networks in personnel selection: a survey of human resource professionals* [Paper Presentation]. 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), Sevilla, Spain. https://doi.org/10.23919/CISTI49556.2020.9140854

Pike, J. C., Bateman, P. J., & Butler, B. S. (2017). Information from social networking sites: Context collapse and ambiguity in the hiring process. *Information Systems Journal*, *28*(4), 729–758. https://doi.org/10.1111/isj.12158

Reda, A. (2019, June 18). *HR Best Practices VS Best Fit*. LinkedIn. https://www.linkedin.com/pulse/hr-best-practices-vs-fit-ali-reda

Reicher, A. (2013). The background of our being: internet background checks in the hiring process. *Berkeley Technology Law Journal*, *28*(1), 115–153. https://www.jstor.org/stable/24120611?seq=1

Rosen, P. A., Solomon, S. J., McLarty, B. D., Esken, C. A., & Taylor, E. C. (2018). The use of Twitter profiles to assess personality and hireability. *Journal of Managerial Issues*, *30*(2), 256–272. https://doi.org/10.5465/AMBPP.2014.17496ABSTRACT

Sameen, S., & Cornelius, S. (2013). *Social Networking Sites and Hiring: How Social Media Profiles Influence Hiring Decisions* [PDF]. Journal of Business Studies Quarterly. https://www.joycerain.com/uploads/2/3/2/0/23207256/social_networking_sites_and_employers.pdf

Samur, A. (2018, November 22). *The history of social media: 29+ key moments*. HootSuite. Retrieved February 2, 2021, from https://blog.hootsuite.com/history-social-media/

Workplace Fairness. (2020). *Social media in the workplace - state laws*. Retrieved February 2, 2021, from https://www.workplacefairness.org/social-media-state-laws

Yeung, C. (2019, August 29). *Social media usage statistics by age: Marketing to adults aged 50+*. Synthesio. https://www.synthesio.com/blog/social-media-usage-statistics-by-age/