Industrial and Organizational Psychology (2022), **15**, 382–384
doi:10.1017/iop.2022.37

CAMBRIDGE
UNIVERSITY PRESS

COMMENTARY

The business of cybervetting

Kristine M. Kuhn

Washington State University—Management, Pullman, Washington
Email: kmkuhn@wsu.edu

Although Wilcox et al. (2022) are correct that cybervetting of job candidates is most often "unofficial and casual," some employers contract with outside firms to conduct online and social media screens as part of the background-check process. Notably, these background-checking firms also market the continual monitoring of existing employees' online presence; cybervetting is not necessarily restricted solely to the hiring process. Although cybervetting as a business-to-business service is relatively uncommon, it may become more widespread if it is perceived as a cost-effective way to mitigate potential risks. This commentary discusses the nature of third-party cybervetting and how outsourcing this process can address some of the concerns raised in the focal article while potentially exacerbating others.

Background-checking firms that offer cybervetting use artificial intelligence to flag problematic social media posts and internet content. For example, Fama Technologies (2022) advertises that it helps employers "surface a range of harmful behavior at the point of hire to protect your business and reduce workplace toxicity." Good Egg (2022) advises employers to consider monitoring the social media of current employees because it can "alert you of any issues that come up over time (like potentially illegal activity, sexually explicit material, demonstrations of racism/intolerance, and so forth)." Wilcox et al. (2022) are appropriately skeptical as to whether personality profiles derived from algorithmic analyses of social media data would predict job performance, but they do not mention the screening services considered here for which predictive validity is not necessarily the appropriate criterion. Someone who is flagged for racist social media posts may or may not behave badly in the workplace, but if such posts are publicly available some risk (however small) is posed to the employer if coworkers or other stakeholders learn of them.

From the perspective of an applicant or employee in the United States, one advantage of outsourced cybervetting is that employers are then subject to the requirements of the Fair Credit Reporting Act. Although ad hoc cybervetting by hiring managers does not require informing targets, an organization that pays a commercial vendor to conduct any type of background check, including online and social media screens, must get written permission from the applicant or employee. That individual also has the legal right to a copy of the report if any adverse action is based on it and can then challenge the accuracy of information or at least become aware of the issue. Conversely, if a hiring manager or human resources (HR) staff employee conducts a search and mistakenly confuses a job applicant with someone else's troubling online presence, there is no obligation to even inform the applicant that is the reason they were screened out.

For employers, the fact that background-check firms rely on artificial intelligence and algorithms offers the potential for cheap, fast cybervetting. As mentioned by Wilcox et al. (2022), some evidence suggests that over time hiring managers have come to perceive unofficial cybervetting as more time consuming and burdensome. The technology used by background-check firms can quickly and cheaply scan enormous amounts of information on platforms like Twitter and Facebook, as well as news sites and other webpages. Their other main selling point addresses the concern that cybervetting could lead to bias and workforce homogenization; these services promise to redact sensitive information regarding protected-class status from provided reports so that client employers do not view it. Outsourcing cybervetting might also make it less likely for hiring managers to be swayed by learning of nonprotected but irrelevant information such as an applicant's hobbies.

The accuracy and usefulness of the information on commercial background-check reports, however, are open to question. In 2020 screenshots of seemingly innocuous tweets flagged by Fama as problematic went viral on Twitter after one employee requested a copy of his own report (conducted after his employer changed payroll vendors) and posted highlights (Heilweil, 2020). Fama reports now provide clients copies of flagged content but do not explicitly label them as good or bad (Heilweil, 2020). If employers are left to make their own judgments, the lack of context or their own biases may still lead them to make erroneous inferences from provided reports. But credit and criminal history reports often contain errors as well, and there is a great deal of variation in how individual decision makers respond to the information contained on these more conventional background reports (Kuhn, 2019).

Moreover, there is no question that many people continue to publicly post information and comments online that could give current or prospective employers pause. The Plain View Project examined[1] the public Facebook accounts of over three thousand current and retired police officers from eight departments across the United States and found about 20% had made posts or comments classified as bigoted and/or likely to undermine public trust in the police (Hoerner & Tulsky, 2019). It is not difficult to find examples of bad hires that might have been prevented by screening online information. For example, one news story with the headline "Cursory Google search would have caught red flags in Spokane school resource officer hire" (Vestal, 2019) notes the officer in question passed the standard background check and had no criminal history.

Typical private employers may choose to hire outside firms for cybervetting if they believe the service will provide additional evidence of due diligence while minimizing the potential for discriminatory implementation and evaluation. Conceivably, some employers might also be persuaded this practice would help screen out "toxic" individuals, thereby fostering goals of diversity and equity (although this has yet to be empirically demonstrated).

Paying a commercial vendor to monitor current employees' online presence raises both ethical and practical concerns. Compared with job applicants, employees may be especially likely to perceive such monitoring as invasive and resent it, particularly if even professional online activity can cause an employee to be identified as a retention risk (Gershman, 2017). In addition, employers face a more complicated decision calculus if a background-check firm reports problematic information discovered about a current employee rather than a job applicant. Third-party observers are unlikely to agree about whether and when discipline for off-duty deviance revealed by social media is merited (Cook & Kuhn, 2021). Yet if a flagged employee is retained and subsequently does engage in deviant or harassing workplace behavior, the employer's potential liability may be heightened because they cannot claim ignorance.

To date, the use of background-checking firms for formal cybervetting appears to be relatively rare, but economic and market incentives may increase its prevalence. Because outsourcing cybervetting addresses some concerns (compliance, cost, transparency) while perhaps exacerbating issues of privacy and accuracy, researchers should not overlook this approach to implementing cybervetting.

References

Cook, W., & Kuhn, K. M. (2021). Off-duty deviance in the eye of the beholder: Implications of moral foundations theory in the age of social media. *Journal of Business Ethics*, **172**(3), 605–620.

[1] These researchers used meticulous efforts to ensure accuracy and authenticity, not algorithms.

https://doi.org/10.1017/iop.2022.37 Published online by Cambridge University Press

Fama Technologies. (2022). *About Fama.* fama.io/social-media-background-check/

Gershman, J. (2017, July 27, B1). LinkedIn case tests whether firms can use your data. *Wall Street Journal.*

Good Egg. (2022). *Social media background checks.* https://www.goodegg.io/social-media-screening

Hoerner, E., & Tulsky, R. (2019). *Cops around the country are posting racist and violent comments on Facebook.* Injustice Watch. https://www.injusticewatch.org/interactives/cops-troubling-facebook-posts-revealed/

Heilweil, R. (2020, May 11). *Beware these futuristic background checks.* Vox/Recode. www.vox.com/recode/2020/5/11/21166291/artificial-intelligence-ai-background-check-checkr-fama

Kuhn, K. M. (2019). Is it disqualifying? Practitioner responses to criminal offenses in hiring decisions. *Equality, Diversity and Inclusion*, **38**(5), 547–563.

Vestal, S. (2019, February 8). Cursory Google search would have caught red flags in Spokane school resource officer hire. *The Spokesman-Review.*

Wilcox, A., Damarin, A. K., & McDonald, S. (2022). Is cybervetting valuable? *Industrial Organizational Psychology: Perspectives on Science and Practice*, **15**(3), 315–333.

Cite this article: Kuhn, KM. (2022). The business of cybervetting. *Industrial and Organizational Psychology* **15**, 382–384. https://doi.org/10.1017/iop.2022.37