

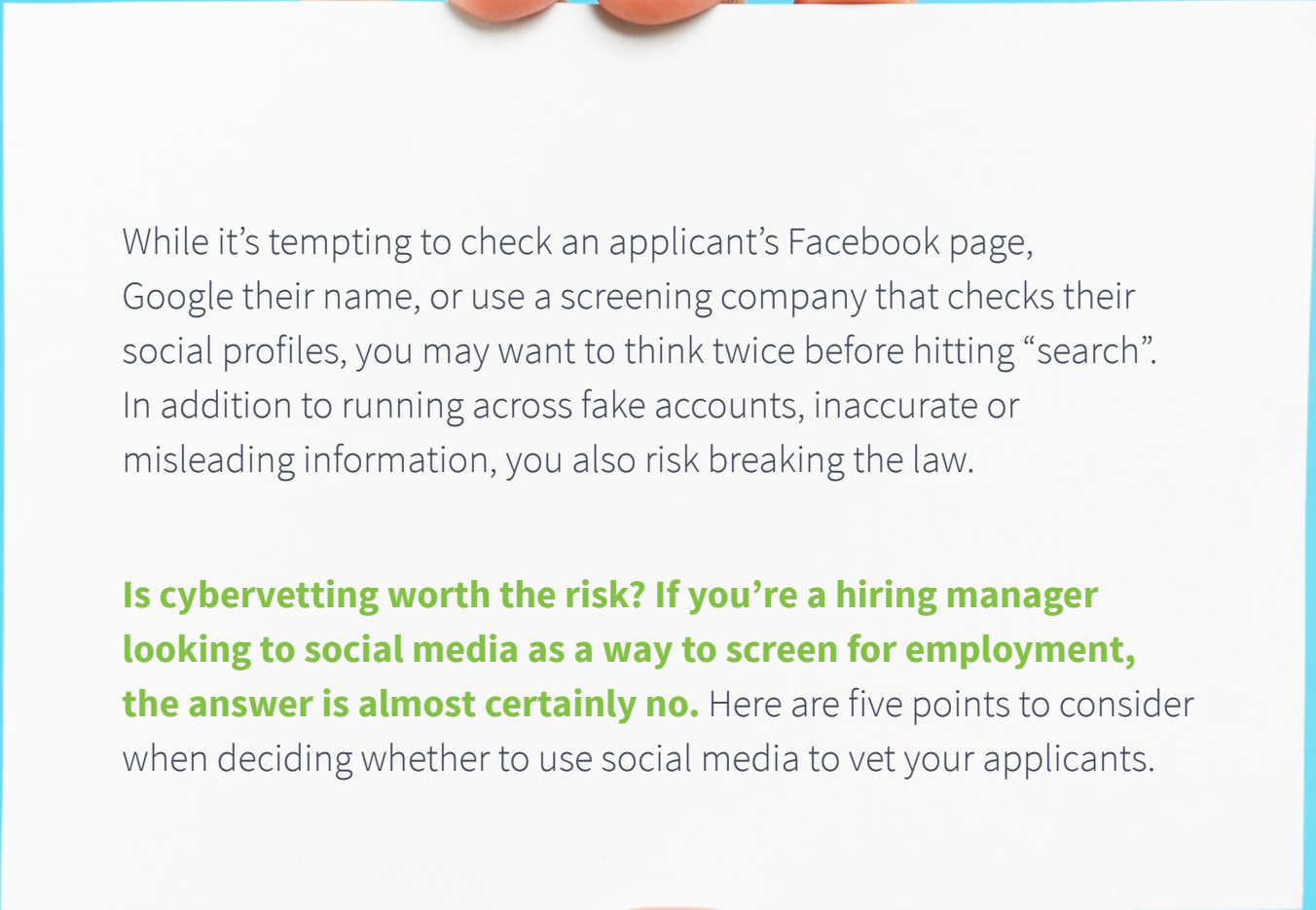


EMPLOYMENT SCREENING DECISION GUIDE

5 REASONS

To Reconsider Using
Social Media Screening During
Your Hiring Process



A hand is shown holding a white speech bubble against a blue background. The fingers are visible at the top and bottom of the bubble. The text inside the bubble discusses the risks of social media screening.

While it's tempting to check an applicant's Facebook page, Google their name, or use a screening company that checks their social profiles, you may want to think twice before hitting "search". In addition to running across fake accounts, inaccurate or misleading information, you also risk breaking the law.

Is cybervetting worth the risk? If you're a hiring manager looking to social media as a way to screen for employment, the answer is almost certainly no. Here are five points to consider when deciding whether to use social media to vet your applicants.

1

False Identity

It's hard to be completely certain that the social media account you're reviewing is owned and updated by the job candidate. **Facebook says between 3 and 4 percent of its user accounts are likely fakes, which means somewhere between 66 million and 88 million fake accounts exist online.**

While email addresses provided by applicants are a great tool in locating your applicants on social media platforms, they aren't always available as an identifier. Your search then has to rely on more general identifiers which may not be unique to the candidate, like city and state, first and last name, and age. Sometimes, the 35-year-old "John Smith" from New York, NY is not the same 35-year-old John Smith from New York, NY who applied to your company.

It's also not uncommon for people to discover "fake" social media accounts that use their own name and likeness.

2

Inaccurate Information

It's difficult (and maybe unwise) to place any confidence in the accuracy of information shared on social media. With account hacking and sharing of accounts by more than one person, you can't be certain that information posted or shared was posted or shared by the person you're interested in hiring.

You also can't be sure that what's shared is true. If we've learned anything in the past year, it's that social media makes it easy to quickly spread false information. It's fairly common for people to intentionally post or share misinformation about themselves or their views as a means to provoke reaction, create dialogue, or to "troll" other social media users.

Things can go viral, and many people can jump into a conversation and change its direction, making it difficult to gauge, let alone understand, the context. In other words, taking information at face value may not give you an accurate impression of the user.

The bottom line is that it's tricky to know if the social media profile you're looking at is factual, that the information was posted by the applicant, and that it carries the meaning you assign to it.

FACEBOOK ESTIMATES THERE ARE BETWEEN

66 MILLION & 88 MILLION FAKE ACCOUNTS

3

Restricted Hiring Criteria

The most significant risk area comes with the availability of impermissible subject matter. Most information shared on social media is innocuous, but you do get routine glimpses of characteristics that are protected under federal law.

For example, Title VII of the Civil Rights Act of 1964 makes it unlawful for an applicant to be denied employment due to race, religion, national origin, or sex. Other laws such as the Americans with Disabilities Act (ADA) and Age Discrimination in Employment Act (ADEA) prohibit denial based on disability and age (40 years or older), respectively.

It's unlawful for an applicant to be denied employment due to:

- **Race**
- **Religion**
- **National origin**
- **Sex**
- **Disability**
- **Age**

That kind of information often appears as part of an online social profile. Even though a person may choose not to fill in those fields or display them publicly, photos and other shared information can very easily expose details about these characteristics.

As a hiring manager or employer, you could argue that mere access to this restricted information doesn't create liability under federal law when you decide not to hire a candidate. You can insist that things like race, religion, national origin, or gender were not taken into consideration during the hiring process.

But if the person denied employment decides to file a civil suit as a result, you'd have to go to trial. Proving that you did or didn't take the restricted information into consideration is a fact-based argument that would require a jury determination.

Take the example of *Gaskell v. University of Kentucky* (5:09-cv-00244). Gaskell, an applicant who was denied employment as a scientist at the university, argued that the university accessed his personal website, which they admitted to doing. He claimed that the religious beliefs expressed on his site lead to the decision not to hire him. The court was very clear in its position that such an issue could not be decided on summary judgment and would require a jury determination. The result? A \$125,000 settlement for Gaskell.

The Equal Employment Opportunity Commission (EEOC) has been vigorously enforcing Title VII lately, especially as it relates to pre-employment screening.

After receiving a great result in *EEOC v. BMW*, in which the auto manufacturer agreed to pay out \$1.6 million to a class of aggrieved employees and agreed to a number of other stipulations imposed by the EEOC, the Commission is continuing its close scrutiny and enforcement of nondiscrimination laws. Employers should also be mindful of this when using social media to screen applicants.

Even if protected information isn't used in the decision, checking the candidate's social media profiles makes it undeniable that you had access to that information. This releases the proverbial genie from the bottle.

There will almost always be a triable issue of fact as to whether protected characteristics were a factor in an adverse hiring decision. It's hard to demonstrate that such information is removed from the minds of the decision makers prior to the hiring decision.

4

Social Media Screeners Are Consumer Reporting Agencies

Many employers who search social media sites think they're safe from the FCRA, which covers employment background checks performed by consumer reporting agencies (CRAs). As long as they're conducting the searches on their own, they're typically right.

The FCRA only applies if an employer obtains its information from a CRA. If you're using social media screening services, however, be careful. These providers are most certainly CRAs that fall under the purview of the FCRA. **Not only are these screeners obligated to follow the FCRA, but their users are, too.**

If you use a third party to perform social media screening services in the employment context, make sure that the provider follows FCRA regulations. That means they have to take steps to ensure maximum accuracy. You'll also want to make sure the screening provider is aware of any state laws that may further restrict what information may be reported and for how long.



5

State And Local Hiring Laws

State and local hiring laws apply to cybervetting, too. For example, some jurisdictions require companies to notify candidates of the specific information in their background reports that led to a denial in employment.

In addition, under federal law, all information reported must be shared with the candidate should an employer decide to take adverse action (for example, not to hire). **This means your use of a candidate's social media profile won't be a secret.** The candidate will know what specific social media information was accessed, which could prompt questions of discrimination in the candidate's mind or attract the attention of the EEOC.

Many state and local laws create a strong case for applicants who are denied after a social media screen is performed. Ban-the-box laws, for example, routinely require that an employer make a conditional offer or perform an interview prior to running a background report.

If the interview goes well enough to warrant a subsequent background report, it's difficult for the employer to argue that the social media information reported was not a factor in an adverse decision. It's then very easy for that denied applicant to make one of two claims:

- If the employer cybervetted the applicant, the candidate can claim the employer had access to protected characteristics under Title VII and that information influenced the hiring decision.
- If a third party social media screening service performed the check, then the candidate could raise questions about the accuracy, completeness, and current nature of the data. When contributing to an adverse action, these factors provide a basis for an FCRA claim.

More Access. More Exposure. Be Prepared.

Some employers will continue to cybervet applicants when making hiring decisions. While there may be benefits to the detailed glimpse into the lifestyle, decorum, personality, and views of applicants, there are considerable downsides—and risks. With more access comes more exposure to protected information. And when using a third-party social media screener, FCRA obligations are triggered.

The accuracy and necessity of social media information will continue to be debated. Savvy employers will consider the risks involved in such screening and determine whether those risks are worth the reward.



DISCLAIMER: The resources provided here are for educational purposes only and do not constitute legal advice. If you have questions regarding your background check process, we advise you to consult legal counsel.



GoodHire's value-packed background check platform is unparalleled.
Find out what we can do for your business.

TALK TO SALES | sales@goodhire.com | 855.496.1572



GoodHire provides customizable background screening services for businesses of all sizes. Through innovative, secure technology, integrations with leading HR platforms, and built-in compliance workflows, GoodHire speeds and simplifies the background check process to help customers build teams based on trust, safety, and fairness. Its award-winning platform empowers applicants to take ownership of their information, and enables employers to make individualized assessments for fair hiring decisions. GoodHire is owned and operated by Silicon Valley-based Inflection, a leader in trust and safety solutions since 2006. © 2019 GoodHire. All Rights Reserved.