Employers Turn to AI to Screen Candidates' Social Media: Best Practices to Minimize Legal Threats

Insights
2.09.26

Roughly 70% of employers now screen social media profiles as part of the applicant screening process – but manually scrolling through Facebook posts, X feeds, and Instagram photos is time-consuming and inconsistent. Enter social media AI investigations tools that promise to streamline the process. These platforms use natural language processing (NLP) to scan candidates' public posts, analyze language patterns and sentiment, and generate personality assessments predicting traits such as teamwork, openness, adaptability, or leadership potential. The pitch is compelling: get deeper insights into candidates' "real" personalities beyond what resumes and interviews reveal, all while saving your HR team countless hours. But before you deploy AI to comb through applicants' social media, you need to understand the significant legal risks these tools create and consider some best practices.

Risks of Social Media Sweeps

Like all tools, use of social media AI investigations tools comes with risks.

Bias and False Inferences

There is a real risk of bias and the creation of false inferences. False inferences can be caused by things such as cultural or linguistic styles, code-switching, slang, sarcasm, and memes, all of which could lead to misclassification by NLP. And bias can arise when "proxy" signals (follows, networks, location) are analyzed, as they can reveal or stand in for protected traits.

Privacy Issues

There are numerous privacy, transparency, and consent concerns to consider. Some state comprehensive consumer privacy laws and a patchwork of AI laws may require notice, choice, or assessments. Global job applicants can also implicate international laws, such as the GDPR, which requires lawful basis, transparency, and DPIA, and has restrictions on special-category data.

Biometric Concerns

Additionally, social media AI investigations tools can raise biometric issues (if the tools use facial analysis). Some states require express consent (e.g., BIPA) and others have password protection laws which restrict requesting account access.

Robotic Limitations

Current limitations of social media AI investigations tools also pose accuracy, authenticity and context concerns. In their existing iterations, AI tools don't understand context or sarcasm and are at risk of misreading humor, quotes, or historical posts. They are also vulnerable to false positives as a result of impersonation/deepfakes, wrong person matches, or stale content.

Discrimination Potential

Reviewing social media feeds can reveal religion, disability, pregnancy, age, political views, and a host of other protected factors that should not be considered at the time of hire. And when utilizing social media AI investigation tools, knowledge of these factors could be imputed to the employer, which may end up tainting employment decisions.

Fair Credit Reporting Act

Even if a third party supplies a "social-media report," it may trigger the FCRA and the requirements that go along with it: disclosure, authorization, pre-adverse/adverse action, dispute process, and accuracy duties.

Data Security

Social media AI investigations tools can also pose security and retention risks. Scraped data creates breach and litigation risk.

Miscellaneous Laws

Finally, off-duty conduct/lawful activities protections (state laws) and whistleblower protections may apply to situations where you monitor social media posts. Employers may also have a hard time proving outputs are job-related and consistent with business necessity.

Best Practices to Consider

There are a variety of ways to mitigate the risks posed by social media AI investigation tools.

Define a Clear and Lawful Purpose

Before implementing social media screening, document the specific job-related reasons for the review and what types of information are relevant to the position. Avoid vague justifications like "culture fit" or "overall personality. Instead, identify concrete traits or red flags (such as evidence of violent threats or illegal activity) that have a demonstrable connection to job performance. This documentation will be critical if you need to defend your screening practices against discrimination claims.

Use Third-Party or Firewall Reviewers

Consider having social media reviews conducted by someone outside the hiring chain, either a third-party vendor or an internal compliance professional who isn't involved in the selection decision. This firewall approach can help prevent protected characteristics (like pregnancy, religion, or disability) from reaching hiring managers and influencing their decisions. If you use this approach, ensure the screener provides only job-relevant information to decision-makers, not raw social media content or assessments that could reveal protected traits.

Ensure Compliance with Privacy and AI Laws

Review your screening practices against state comprehensive privacy laws (like the California Privacy Rights Act), biometric privacy statutes (like Illinois BIPA if facial recognition is involved), and emerging AI-specific regulations such as New York City's Local Law 144. If you're hiring international candidates, ensure compliance with the GDPR, which requires transparency, a lawful basis for processing, and potentially a Data Protection Impact Assessment. Document your legal analysis and update your candidate privacy notices to disclose that social media may be reviewed as part of the screening process.

Validate and Document Job-Relatedness

If your AI tool produces scores or assessments based on social media data, treat it like any other employment test: it needs to be validated to show it actually predicts job performance and doesn't create disparate impact. Work with industrial-organizational psychologists or your FP counsel to conduct validation studies, particularly if the tool measures subjective traits like "adaptability" or "leadership potential." Without documented validation, you'll struggle to prove business necessity if the tool disproportionately screens out protected groups.

Train HR and Decision-Makers

Ensure everyone involved in social media screening understands what they can and cannot consider, how to avoid bias, and when to escalate concerns. Training should cover how to recognize protected characteristics that should be disregarded (such as religious posts or photos suggesting pregnancy), the risks of making inferences based on networks or affiliations, and the importance of consistency across all candidates. Decision-makers should understand that AI-generated assessments are tools to inform judgment, not replacements for human evaluation.

Provide Transparency and Due Process

Inform candidates that their public social media may be reviewed and give them an opportunity to explain potentially disqualifying content before making a final decision. If you discover information that would lead to an adverse decision (such as posts suggesting illegal activity or workplace policy violations) give the candidate a chance to provide context. After all, the post could be satire, a quote, or simply misunderstood. This approach not only reduces legal risk but also improves candidate experience and protects your employer brand.

Follow FCRA Procedures (If Applicable)

If a third party conducts the social media review and provides you with a report bearing on the candidate's character, reputation, or personal characteristics, the review could trigger FCRA requirements. This means you must provide candidates with a standalone disclosure, obtain written authorization before the review, and follow pre-adverse and adverse action procedures (including providing a copy of the report and a summary of rights) before rejecting them based on the findings. Consult with your FP counsel if you're unsure whether your vendor relationship triggers FCRA obligations. NOTE: the recent Eightfold AI lawsuit demonstrates that courts may interpret these requirements broadly when AI tools are involved.

Limit Data Collection and Retention

Only collect and retain social media data that is necessary for the screening decision, and establish clear retention schedules. Avoid scraping entire social media profiles or maintaining permanent databases of candidate information, as this increases your exposure to data breach litigation and privacy violations. Once a hiring decision is made, delete or anonymize social media screening data unless there's a legitimate business reason to retain it (such as defending against a discrimination claim).

Conclusion

We will continue to monitor developments related to AI hiring tools. Make sure you are subscribed to Fisher Phillips' Insight System to get the most up-to-date information. If you have questions about your organization's use of AI in recruiting or hiring, contact your Fisher Phillips attorney, the authors of this Insight, or any attorney in our AI, Data, and Analytics Practice Group, our Privacy and Cyber Practice Group, or our FCRA and Background Screening Practice Group.

Related People

Kile E. Marks, FIP, CIPP/US, CIPM, CIPT
Associate
858.964.1582
Email

Richard R. Meneghello
Chief Content Officer
503.205.8044
Email

David J. Walton, AIGP, CIPP/US
Partner
610.230.6105
Email

Service Focus

AI, Data, and Analytics

Privacy and Cyber

Employment Discrimination and Harassment

FCRA and Background Screening