Legal Considerations when Using AI in Recruitment: An Executive Summary

impress

At impress.ai, we are committed to increasing fairness in the hiring process and see our solution as a key driver of this all-important goal. However, we recognize that with disaggregated global regulation around AI technology, it's essential for organizations to understand the legal considerations and how to best use the technology to drive compliant and positive outcomes.

Introduction

impress.ai recently commissioned a research whitepaper from Shloka Vidyasagar for industry professionals looking for practical advice on the legal considerations of leveraging AI for recruitment.

This document summarizes its findings, providing insights that any organization can apply when implementing AI in recruitment. In addition, it highlights how impress.ai is responding to this growing challenge.

Readers are invited to download the complete research whitepaper here.

Current Landscape and Dynamics

The use of automated decision-making software has grown exponentially in the last decade due to its significant accuracy and efficiency benefits. However, as the practice has expanded, an unprecedented collection of legal issues has arisen along with it, making compliance on behalf of industry practitioners ever more nuanced.

Key Technologies and Legal Considerations

Technology	Key Legal Considerations
 **AI Matching Technologies** AI matching technologies are typically used to evaluate potential candidates on role-based criteria. They increase efficiencies and avoid human bias to create the best longlist based on the ability to perform the job alone.	Because these technologies learn from existing data sets, ingrained and historical biases at an organizational level can taint them. Algorithms learn from this data, with the potential to replicate and amplify existing biases, regardless of any other emphasis placed on merit. This presents a significant risk of inadvertently increasing discrimination in hiring and contravening employment law.
 **AI Chatbots** AI Chatbots are an efficient way to discern a candidate's compatibility, leveraging algorithmic and learning-based response technologies to act as an objective interviewer or responder to FAQs.	Privacy watchdogs are increasingly monitoring the use of AI Chatbots in relation to privacy and employment laws. There is a prevailing concern that these tools can access information about a candidate that would be unattainable by human evaluation, using it to make hiring decisions. Therefore, upholding the privacy rights of candidates is critical and must be considered in building your chatbots.
 **AI-Grading Software** AI-grading software automates the grading of applications throughout the recruitment process, from candidate compatibility to evaluating interview responses.	While functionally similar to AI-matching technologies, these grading software bears different legal considerations. In the pre-employment phase, there is a privacy concern that the algorithms may discern information that human analysis could not. Furthermore, there is a risk that algorithmic solutions can have their own biases at all stages, stemming from a lack of human empathy, social awareness, and critical reasoning skills to make equitable assessments.
 **Facial Recognition and Voice Analysis** These technologies use biometric attributes to determine information about a candidate that was previously unattainable. During the interview phase, they are commonly used to derive additional insights from facial expressions, body language and verbal language choice, style and tone.	Existing employment laws were not designed to govern these technologies, hence are difficult to adapt. Furthermore, their use raises significant privacy concerns, as biometric data handling requires additional safeguards, and collection can be considered invasive. In addition, the process may be tainted by discriminatory algorithms, creating a complex employment law concern. In its infancy, facial recognition was primarily developed based on Caucasian males. This can add inherent bias as these were the first traits embedded by machine learning, demonstrated by a reported 34% increase in bias when analyzing women of color. [1]

1 The Gender Shades Project, http://gendershades.org/overview.html

Key Insights for Industry

Measuring Efficacy

- The efficacy of AI solutions must be measured within the broader context of the organization's goals and prevailing employment laws.
- In addition, intelligent decision-making systems should be routinely assessed by accredited bodies to ensure they remain in line with prevailing legislation.

Regulating Bias

- Algorithms learn from existing data and can replicate existing biases if unsupervised.
- Biometric tools, such as facial recognition can carry machine-learned biases that can have a notable impact on candidates based on gender and race. Therefore, it is critical to be aware of this potential and consider insights from these tools alongside human interaction with the candidate.

Upholding Privacy

- Any AI solution must be built to stringent privacy by design principles to uphold candidate privacy rights and protect the organization from privacy or employment law breaches.
- Upholding privacy requirements is often thought of as simply collecting informed consent, such as via agreement to an online disclosure statement. However, as these disclosure statements become more and more complex, a legal argument has emerged around 'infoxication'. Infoxication refers to information overload, creating a point at which an average person could not give informed consent because it is conceivable that they don't understand what they are agreeing to.
- The use of just-in-time notices is increasingly being considered best practice, as the model facilitates informed consent through increased accessibility of information. These notices work by providing a series of smaller, contextualized and more easily digestible disclosures for review and consent just before each piece of data is collected.
- Biometric data used for employment purposes can be considered a breach of privacy where the information it derives was not voluntarily provided to the employer.

Safeguarding Biometric Data

- Biometric data requires an extra level of protection as there is a higher threshold involved with handling data, and misuse can bear significantly more repercussions.
- For those in jurisdictions governed by the General Data Protection Regulation (GPDR), it's important to note that this legislation puts biometric data in the special protection category. This means that the processing of biometric data is prohibited without the subject's specific consent.
- Best practice in this area can be taken from healthcare technologies, which have long been built to stringent privacy design principles with special protections built in for biometric data. These technologies are often governed by local legislation, such as HIPAA in the United States or the Privacy Act 1988 in Australia.

In Summary

The use of AI in recruitment poses a rapidly emerging legal challenge. Without comprehensive legislation governing the technology, the onus is on industry practitioners to apply traditional legal doctrines to complex systems.

In relation to employment law, the primary concerns revolve around bias in algorithms. A large part of this risk is rooted in misguided and unsupervised mandates. Unsupervised learning systems that learn from a pattern of existing biases pose legal and employment concerns when used for recruitment purposes.

It is incumbent upon organizations to ensure their algorithms are supervised, based on recognized organizational psychology principles, and routinely assessed.

Concerning privacy, technology presents a novel consideration to the right to privacy itself. Advancements in artificial intelligence offer opportunities to collect data that was previously unattainable. In this landscape, organizations must have a compliant means to collect privacy consent, ensuring notifications are easily accessible, comprehensible, and up to date.

When there is no legal requirement to institute such measures at the time of writing, proactivity might provide practitioners with retroactive indemnity and a competitive edge.

The impress.ai response

At impress.ai, we employ a combination of rules-based and supervised learning algorithms. Our approach sets rules based on widely recognized organizational psychology research that demonstrably combats bias. It does this by evaluating the candidate's merits within a prescribed mandate rather than replicating potentially problematic hiring norms.

In addition, we can help HR and recruiters refine and build the best privacy consent structure for their system and jurisdiction, including traditional notifications and just-in-time notices.

We also recommend and support impress.ai clients to seek bias assessments from accredited bodies. Just as an organization would perform employee evaluations, assessing intelligent decision-making systems should be routine to ensure their mandate remains impartial and in accordance with prevailing regulations.

impress

Interested in more information?

Contact impress.ai

contact@impress.ai

impress.ai

Head Office, #08-01, 80 Robinson Road, Singapore- 068898