THE JOURNAL RECORD

Gavel to Gavel: Biometrics in the workplace

By: David Limekiller Guest Columnist March 27, 2019 0

David Limekiller

Biometrics has a long history of use in the workplace. However, as biometric technology continues to improve, it has become a valuable and efficient tool for employers.

Common uses through fingerprints, retina and facial recognition include timekeeping, electronic security and building and accessing workplace equipment.

The use of biometrics in the workplace is an evolving area of employment law and this uncertainty presents challenges to an employer's efforts to implement proper procedures for a biometric program. No single federal statute establishes specific guidelines regarding an employer's obligations pertaining to the collection, use, or retention of biometric information. Only several states have passed laws to regulate biometric privacy in the workplace.

Oklahoma has not enacted any statutes or regulations regarding biometrics in the workplace. However, the absence of statutory authority does not protect an employer from claims regarding biometric data.

An employer is still subject to common law claims such as right to privacy or negligence relating to how an employee's biometric data is collected, protected, used, displayed, or retained. Employers are recommended to work with counsel to create policies and procedures to minimize potential liability. The policies should provide full disclosure to the employees regarding the use and disclosure of their biometric information so that employees can give their informed consent to the employer.

To avoid and defeat any right to privacy claims, it is suggested that any policy for any biometric system include:

- Clearly inform your employees why the biometric system is needed.
- Obtain written consent from employees and specify the permitted uses.
- Develop alternative policies to accommodate employees who refuse to participate or are unable.
- Do not sell, license, or transfer any biometric data to any third party without the employee's prior written consent.
- Protect the biometric data to the same degree you protect your other confidential information and use encryption if possible.
- Develop and communicate a written policy on retaining and destroying biometric data.
- Ensure there are no disclosures of biometric data to any third parties without employee consent, or as required by law.
- Any disclosure of biometric data to law enforcement shall be through a warrant or subpoena.

- Create a plan to respond to a data breach.
- Have counsel review all contracts with any third parties who will have access to the biometric data to ensure that the biometric data will not be disclosed or misused.
- Work with counsel to monitor developments in the law.

David Limekiller is an attorney with GableGotwals practicing in the areas of banking, health care, and labor and employment law.

---

https://journalrecord.com/2019/03/27/gavel-to-gavel-biometrics-in-the-workplace/