

Is It OK To Fingerprint Your Employees?

The use of biometric technology for timekeeping in the construction industry brings with it some labor and legal pitfalls

May 3, 2017 by Clare M. Gallagher

Biometric technology measures genetic characteristics, such as fingerprints, iris or retina patterns, facial characteristics and hand geometry and can provide companies with a new way to ensure that individuals are who they say they are.

For example, banks in foreign countries now allow customers to scan their fingerprints at ATMs, instead of requiring the use of a bank card and an easy-to-crack four-digit code. Similarly, biometric technology provides employers with an opportunity to guarantee the right person is punching the time clock, thus preventing employee time fraud.

Proponents note that, since biometric markers are unique to each individual, they provide a more reliable means of verifying identity or, say, providing access to secure sites than traditional IDs, such as badges or password-based systems. However, the collection of biometric information has raised civil rights and privacy concerns.

Despite that, the use of biometrics in the construction industry has broad appeal. When tracking a mobile workforce on a large jobsite, the logistics are complex. Contractors need to know exactly who is working where and when and for how long. For example, without accurate timekeeping records of their own employees and those of their subcontractors, as required by the Davis-Bacon Act, federal contractors may be subject to fines and additional liability.

Unfortunately, contractors have had limited guidance in their implementation of biometric time-keeping systems, and the law as it pertains to collection and storage of biometric information is still evolving. Firms that are considering the use of biometric information to track employees' time should be aware of the legal implications for their companies and subcontractors.

First, contractors who employ union workers should keep in mind the firm's duty to bargain in good faith before implementing biometric timekeeping. Although the National Labor Relations Board appears to be receptive to the new technology for use in timekeeping, recent NLRB decisions have cautioned that employers must bargain with a union under certain circumstances.

Contractors must bargain when it is clear that, among other things, the new system will subject unit employees to additional discipline or increased oversight. When either of these conditions

obtain, employers are generally not permitted to implement biometrics unless union representatives agree to its use or the parties have reached an impasse.

Statutory Protections

Less clear are the statutory limitations that may be imposed on contractors that use this type of system. Some states have statutory protections for employees with respect to the use of bio-metric technology. For example, New York expressly prohibits employers from requiring employees to be fingerprinted as a condition of employment.

Additionally, some states have placed conditions on a private or commercial entity's collection and use of biometric information, based on informed consent from the individuals from which it will be collected. Those states also provide guidance about the storage and destruction of collected information. A number of states also require the collection entity to provide, at the very least, notice to individuals that a security breach has occurred.

Other states, including Pennsylvania and Ohio, have yet to address the use of biometric technology in the workplace. Interestingly enough, however, even in states without laws governing its use, contractors may face additional obstacles to biometric timekeeping. One West Virginia federal court decision, for example, found that an employee whose religious views conflicted with an employer's use of biometric technology was entitled to a religious accommodation under federal antidiscrimination law.

Even if your firm is operating in a state that does not prohibit the use of biometric information, a best practice is to obtain consent for its collection, secure the information properly and dispose of it appropriately. Differences often arise between the contractor and the individuals whose information is being collected: the requirements for consent, the length of time biometric information may be stored and protocols for its destruction.

In light of these uncertainties, contractors should consult with legal counsel before implementing any type of biometric timekeeping system.