Using Biometrics In The Workplace

Insights
1.06.14

(Labor Letter Update, January 2014)
In the past, employees rarely objected to having their picture taken for the company's identification badge. But in this age of technology allowing for facial recognition, photo "tagging," finger or palm prints, and other biometrics – even including DNA – employees often resist requests for personal information to be used in connection with security or other business needs.

"You Want My What? Why?"
Some employers are using biometrics in an attempt to better establish records of employee hours worked. With the increase in cases where employees have coworkers clock them in or out of work ("buddy punching"), and fraudulently recording inflated or inaccurate hours worked, employers have turned to new technology to reduce such fraud.

Additionally, employers desiring to avoid potential claims of failure to properly pay compensation including overtime, are looking for more accurate and reliable ways to determine whether an employee was actually present (or perhaps was not present) in the workplace at any given time.

Employers are also looking for better ways to provide for security and restrict access to specific areas in the workplace, and to be able to know which individuals were present in specific workplace areas at any given time. For remote tracking of employees, GPS devices have been used for some time to allow an employer to know the location of a company vehicle or specific employee.

GPS tracking has often been challenged as too invasive, but has generally become an accepted manner for employers to keep track of employees and company property. With improvements in technology providing for secure "keyless" locks based on biometric data from individuals authorized to access a facility or office area, employers can now track access and activity with more accuracy.

Finally, some employees are receiving notices from their employer in accordance with provisions of the Affordable Care Act regarding the availability of free biometric screening. It has been reported that such biometric screening by employers could become mandatory in the not too distant future.

While many employees may think this sounds Orwellian, employers know that the need for security in the workplace is more important than ever. Many have praised the use of biometrics for enabling them to keep records of their employees' time more accurately, and increasing the security level at employer facilities by making it more difficult for nonemployees to gain access to the facility.

Employees are therefore being asked for more information more often, and have begun to question what else an employer might be able to do with such data. There have been fears that the data could be compromised, stolen or misused, leading to all kinds of mayhem.

"And What If I Refuse?"

As you can imagine, there has been significant backlash from workers of companies who have implemented biometric systems. A few years ago in New York City, the Bloomberg administration implemented biometrics technology to keep track of city employees. This was met with contentious reactions by employees. Many workers expressed outrage that the system was intrusive and violated their privacy interests. But overall the city was very pleased with the results of the system and proclaimed it to be the "wave of the future."

So with a "Just Say No" mentality, employees who fear the possible misuse of their private data, or who object to what they view as the ultimate invasion of privacy, are refusing to allow an employer to scan, record, collect or otherwise obtain biometric data. This raises the question of what the employer can and should do.

The employment-at-will doctrine allows employers to terminate employment for any lawful reason (whether good or bad). Absent legislation providing that an employee cannot be fired for refusing to provide a fingerprint, iris scan, or other biometric data, an employer would certainly have the right to terminate the employment of any individual who refuses to hand over their data. But from an employee relations point of view, *should* an employer do so?

Consider what happened when some employers started collecting social-media passwords or other such information from employees and applicants. Public outrage quickly led to legislation in many states to address such an invasion of personal privacy. Also consider the laws passed in response to the use of social security numbers by employers for identification badges or computer access purposes, and the liability imposed on employers who do not properly maintain the security and integrity of systems and processes containing employee personal information. Often a compromise of such information can lead to identity theft and claims against the employer.

Some other countries, including Canada, require employers who use biometric data to ensure privacy. In the U.S., Illinois has a law regulating the collection and use of biometric data, and New York has a law prohibiting employers from fingerprinting employees unless required to do so by law. Proposed legislation to limit the use of biometric data in New Hampshire was defeated in 2010. There will no doubt continue to be legislative developments in this area, and individuals will look for ways to use these and other laws to limit employer collection and use of biometric data.

Other Legal Theories

Employees can also challenge the use of biometrics based on protected class claims under federal or state laws prohibiting discrimination. In past years, such theories have been used by employees who object to having their photograph taken.

The Equal Employment Opportunity Commission recently filed a lawsuit against Consol Energy Inc., and Consolidation Coal Company in West Virginia alleging religious discrimination in connection with the use of biometric technology for timekeeping. In that case the employee, an evangelical Christian, believed that submitting to a workplace hand scan had a connection to the "Mark of the Beast" as referenced in the Book of Revelation.

The employee asked the company to accommodate his religious beliefs by allowing him to track his time some other way, such as through a more traditional manual time recording system. The company refused, and the employee filed a charge ultimately resulting in the lawsuit.

Employers should be prepared to face such issues in connection with the use of biometrics, and as is the case for any employment policy or practice, should be careful to consider any objection or requests for accommodation when an employee asserts a supporting legal basis for the objection or request.

How Does This Work at Work?

Before we discuss more of the "pros" and some of the "cons" of this system, let's first break down exactly how biometric systems work, specifically when it comes to hand scanners.

First, the biometric time clock scans and captures data from the geometry of the employee's hand. Then a camera in the biometric device takes a picture of the employee's hand and the shadow it causes, using that information to determine the length, width, thickness, and curvature of the hand. Finally, this information is then in turn used by the device to identify the employee.

In other words, no longer will an employee's coworker, supervisor, or anyone else be able to clock that employee in or out of work. The process of using an iris scanner or fingerprint optical scanner is very similar.

As an interesting aside, various hotels across the country have also implemented biometrics for their customers. Instead of the guest using a room key, the hotel would scan a guest's eye or hand for access to the hotel room.

One caveat, however: companies using fingerprint or other biometric data devices (not just for employees but in the case of businesses such as gyms and tanning salons who require customer biometrics for access) have found that the technology is not perfect – often for various reasons the system is down or the scan does not work (because, for example, the individual has a cut on their finger). So it is possible that if a worker cuts his finger, that could alter the fingerprint or the curvature and dimensions of the employee's finger, thus preventing the system from recognizing the print.

Another problem with biometric technology is that individuals have already figured out how to hack and fake biometric data. Reportedly, Apple's new technology using a fingerprint to unlock a device has already been compromised. This problem has led to systems requiring multiple "keys" for

access, such as a fingerprint coupled with a traditional secure identification card. Employers should keep all of this in mind, investigate the technology, and consider all factors in contemplating the use of a biometric system.

Our Advice

Here are a few practical tips any employer should consider before riding the wave into the area of biometric technology in the workplace:

1.Notify all employees, in writing, of the company's intent to use a biometric system –include the reasons, what safeguards will be provided, and what an employee should do if they have any questions or concerns about the system.

2.Check all applicable privacy and other potentially relevant laws before implementing the system (laws on the books in this area can quickly change, as can the interpretation of existing laws).

3.Implement strict security policies and procedures that will ensure all biometric data will be securely stored and safeguarded.

4.If your company is unionized, give the union sufficient notice of your intention to implement the system and verify your right under any collective bargaining agreements to implement such a system.

5.Be ready to consider accommodation or other requests from employees who may raise issues based on disability, religious beliefs, or other areas protected by law.

With new and creative technology increasingly available every day, it is safe to assume that biometric systems in the workplace will become more and more popular. But as with any new technology it will bring new challenges and new opportunities – so as the Boy Scouts say: Be Prepared!

For more information contact either of the authors: CRWright@laborlawyers.com, JWilson@laborlawyers.com, or 404.231.1400.

Service Focus

Privacy and Cyber