The Legal Minefield Surrounding Biometrics In The Workplace

Insights
10.02.20

The use of biometric-enabled devices has become ubiquitous in the modern workplace. Biometric time clocks offer employers an accurate and reliable way to track employees' hours, while increasing accountability. Biometric locks are often ideal for employers protecting sensitive information or valuable property, as biometric authentication reduces the risk of information (i.e., passwords or combinations) or physical tokens (keys or RFID badges) being inadvertently passed on to unauthorized users. In the COVID-19 era, biometric kiosks even offer employers a streamlined method of ensuring employees do not have an elevated body temperature. The benefits of biometric systems are undeniable.

However, businesses also assume risks when they employ biometric systems in the workplace. From a legal perspective, the most widely discussed risk is running afoul of one of the biometric information privacy laws in place in different states throughout the country. These laws typically require specific disclosures be made to employees prior to the collection, use, or storage of biometric data and carry heavy penalties for employers who fail to do so.

But running afoul of privacy laws is not the only risk employers face when implementing biometric systems. This article briefly covers the current state of biometric privacy laws in the United States and assesses the minefield of potentially unforeseen legal issues awaiting unprepared employers who implement biometric systems without the requisite thought or preparation.

Biometric Security Laws
The Illinois Biometric Information Privacy Act (BIPA) is the forerunner of modern biometric information privacy laws in the United States. BIPA was enacted to regulate the collection, storage, and use of "biometric identifiers" and "biometric information." Although the statute was enacted in 2008, it remained dormant until 2015 when class action lawsuits alleging violations of the Act were first filed – primarily alleging violations stemming from social media facial recognition features.

These first cases triggered a tidal wave of litigation targeting employers who used biometric timekeeping and security systems. Penalties for violating BIPA are extremely punitive and, in light of the recent decision in *Cothron v. White Castle System, Inc.*, employers could be liable for in excess of $1,000 per day, per employee, for each day biometric information was collected, stored, or used improperly.

While BIPA is perhaps the most well-known law of its type, it is certainly not the only law employers need to be aware of in this field. In the nation's most populated state, the California Consumer Privacy Act (CCPA) regulates the collection, storage, and use of "biometric information," which is broadly defined. Unlike BIPA, however, the CCPA does not apply to every employer and the most punitive penalties can only be sought by the California Attorney General. Still, failure to comply with the CCPA could result in severe financial and operational repercussions.

Texas also regulates the "Capture or Use of Biometric Identifier." Like its counterparts in Illinois and California, the Texas law prohibits any person from capturing biometric information without informed consent and regulates the storage and use of said information thereafter. "A person who violates the law is subject to a civil penalty of not more than $25,000 for each violation," but enforcement actions can only be brought by the attorney general. Similarly, Washington state prohibits the unauthorized use and collection of "biometric identifiers," but also leaves enforcement actions to the state's attorney general.

In addition to the laws currently on the books, Arizona, Florida, and Massachusetts have all recently proposed bills to protect biometric privacy through legislation. The trend is clear: the number of states with some form of biometric privacy law is increasing. For that reason, it is crucial that you stay up-to-date with laws applicable to each state in which you operate and consider implementing robust, preventive policies.

Legal Landmines In The Biometric Field

It is also critical, however, to not let compliance with privacy laws be the only legal consideration you make before diving into the biometric pool. There are other legal factors you should consider.

Unwitting Indemnification

In addition to defending against possible violations of biometric privacy laws, employers also face the risk of indemnifying the vendors who provide them with biometric hardware and software. Major manufacturers of biometric time clocks, biometric locks, and other biometric devices typically include an indemnification provision in their service agreements. Although the wording of this provision differs from company to company and contract to contract, it typically includes language whereby the employer agrees to defend the vendor against "employment-related claims" or claims "arising out of an employee's use of the vendor's services or products" and hold the vendor harmless for any resulting liability.

Historically, these indemnification provisions applied to situations unrelated to employee privacy, like wage and hour lawsuits. In those situations, it would be uncommon for a plaintiff to not name both the vendor and the employer, or just the employer, as defendants in the lawsuit. Conversely, in the new biometric information privacy landscape, plaintiff-employees have started naming technology vendors as *sole* defendants in BIPA actions. This could be for several reasons.

One possible explanation is that these plaintiffs are attempting to expand the scope of the alleged class beyond one employer. In at least one case, two plaintiffs in the same action worked for

class beyond one employer. In at least one case, two plaintiffs in the same action worked for unassociated employers who, coincidently, used the same biometric timeclock vendor. By naming the vendor as a defendant, it allowed the plaintiff-employees to expand the scope of the alleged class while proceeding jointly in the same action. Other possible motivations include avoiding *res judicata* issues for employers that have already been named in a separate action, mooting employment-based arbitration agreements with class actions waivers, and/or simply targeting the perceived "deep pockets." As litigation surrounding biometric privacy spreads into states outside of Illinois, it is probable that other plaintiffs will take a similar approach for the same reasons.

These lawsuits call into question whether employers should agree to indemnify biometric equipment vendors as to "all employment-related claims" or "all claims related to an employee's use of the vendor's equipment or services." Doing so puts the employer in a position where it could be compliant with all applicable biometric privacy laws, but still pay the costs of defending a lawsuit and all liability stemming from a biometric vendor's failure to comply with those same laws. For instance, a major biometric time clock vendor in Illinois was alleged to have violated BIPA by storing biometric information in off-site data centers hosted by third-party companies without the requisite consent. These alleged violations occurred independent of any action from the employer and, presumably, without the employer's knowledge.

At the very least, before entering into a services agreement with an indemnification provision, you should consider negotiating a specific carve out to biometric and privacy-related claims. Further, all services agreements should include provisions that require biometric vendors to remain compliant with all applicable biometric privacy laws or be individually and solely liable for their failure to do so.

Inadvertent Discrimination Claims Tied to Fingerprint Readers

Fingerprint scanners are the most common form of biometric authentication. Modern fingerprint scanners use light and photocells to digitize the ridges on an individual's fingers or hand and render that data into a "template" unique to those ridges. This is, in essence, a high-tech version of traditional "fingerprinting" that has been used by law enforcement for more than a century. However, not all individuals have fingerprint ridges that allow for such a reading to take place.

While some individuals are born with congenital adermatogyphia – the clinical term for congenital or acquired loss of fingerprint ridges – it is more commonly acquired as a side effect of aging. One study found that only 0.3% of people 24 or younger were affected by fingerprint loss, while 8.5% of those aged 65 years or older were affected. Said differently, as people get older, their fingerprints may not be "readable" because of the loss of definition.

If you encounter a situation where an employee's fingerprint is unreadable, you should be very cautious to avoid any actions that would make that employee feel singled-out or targeted because of their age or physical characteristics. At the same time, you should also be cautious to avoid arranging a system that could be seen as favoritism by other employees who are required to use biometric authentication.

The best solution, if possible, is to use the settings in the fingerprint scanner itself to reduce the biometric threshold for fingerprint recognition as to that employee only. This feature is available on several popular models of fingerprint scanners and will allow for essentially any fingerprint – even on a finger lacking distinct ridges – to be recognized. This will allow for employees with low fingerprint definition to use biometric time clocks and other devices.

However, if the threshold is reduced too far, it could allow for false positives and result in the problems biometrics are implemented to avoid (i.e, "buddy punching"). This can be avoided by simply reducing the threshold when the employee is enrolled in the system for the first time, which lowers the amount of information collected from that employee and need not be disclosed. If employees are then trained to use the same finger to clock in and out, it is probable they will continue using the scanner indefinitely without ever noticing a difference or knowing another fingerprint could also work.

Employees Should Not Be Forced To Use Biometrics If It Contravenes Their Religious Beliefs

Lastly, employees should not be forced to use biometric scanners if it contravenes their religious beliefs. In a high-profile case from West Virginia, the EEOC filed action on behalf of an employee who believed he was denied a religious accommodation related to the use of a biometric time clock. The employee believed that he should not have to submit either of his hands for biometric scanning because it "would make him take on the Mark of the Beast." The employee requested that he be provided an alternate method to clock in, but the only accommodation offered by the defendant was allowing the employee to use his "left hand palm up instead of his right hand palm down."

This was unacceptable to the employee as he claimed it was a violation of his religious beliefs. He thereafter retired "under protest" and initiated legal action. At trial, the jury found that the employer failed to accommodate the employee's religious beliefs and awarded the employee $150,000 in non-economic damages; the judge tacked on an additional $436,860 in economic damages. On appeal, the 4th Circuit Court of Appeals affirmed the trial court's order and upheld the verdict and damages awarded.

For this reason, regardless of what you perceive to be "reasonable" in the context of biometrics, you should engage in an interactive process to determine if you can provide an accommodation if an employee's religious beliefs prevent them from using a biometric device. More broadly, the case illustrates that biometric devices will create unforeseen issues when implemented in a workplace.

While the employer in the West Virginia case cannot necessarily be faulted for failing to consider the possibility that the "Mark of the Beast" would prevent an employee from using its timekeeping equipment, its failure to address the issue properly when it arose resulted in substantial liability. You should take issues surrounding the use of biometric devices seriously and, when necessary, consult with counsel to ensure best practices are being followed.

Conclusion

This article provides a brief overview of some of the issues related to biometric privacy laws but is by no means comprehensive. As the use of biometric technology continues to spread in the workplace additional, presently unforeseen issues will develop. To stay ahead of the curve, you should take active steps to implement policies and review and negotiate contracts carefully with the expectation that your business may be affected. These simple steps will allow you to enjoy the benefits of biometric technology while mitigating the potential risks associated with its use.

For more information, contact the author here.

Service Focus

Consumer Privacy Team

Privacy and Cyber

Employment Discrimination and Harassment

Litigation and Trials