

YOUR FINGERPRINTS, YOUR IDENTITY, YOUR PRIVACY

PROTECTING YOURSELF IN THE WORKPLACE



A White Paper
Presented By

TMF

LAW OFFICES OF
TODD M. FRIEDMAN, P.C.



OUR EXPECTATION OF PRIVACY

Whether we are banking, buying products online or visiting our doctors, we all have a strong expectation that our privacy will be protected. The people with whom we engage in commerce are privy to important personal information: Our health histories, our credit card information and other important pieces of critical personal information are traded frequently.

Biometric privacy is one of the most important forms of privacy that has become a major issue in recent years. Employers, airports, security firms and many other industries are employing biometric data with increasing frequency.

One problem with the increased use of biometric data involves privacy. It is difficult enough for people to protect their personal information; it is nearly

impossible for people to protect their biometric data from theft. Negligent storage of data, inadequate security and other oversights can result in identity theft and other personal rights violations.

In the workplace, biometric privacy is particularly important and difficult to protect. More employers than ever before are using biometrics – in particular, fingerprint authentication – for time-keeping and security purposes.

As with most quickly developing technologies, the law is behind the times when it comes to protecting the average employee and consumer from the dangers involved with the growing use of biometrics.

Currently, Illinois is the only state with a clear legal schema for protecting individual biometric privacy rights, including a private right of action for those whose rights have been violated. California is also developing amendments to its existing information privacy laws. But there is no federal law covering this area, and most states are still developing legal protections for victims of biometric privacy rights violations.

As an employee and consumer, it is critical for you to learn about biometric privacy and how you can protect your rights.

WHAT ARE BIOMETRICS?

Most simply, biometrics is the science of measurements.¹ Biometrics measures, collects, analyzes and uses physical or behavioral characteristics for the purpose of identity authentication.

There are two main categories of biometrics: **physiological** and **behavioral**.

Physiological biometric data includes everything from morphological data like fingerprints, retinal scans and facial scans to chemical data like blood sampling.

Behavioral biometrics include things like voice recognition, signature recognition and movement recognition.

BIOMETRIC PRIVACY OVERVIEW

With the ever-increasing pace of technological developments in our country, biometrics have become a regular part of everyday life for many Americans. Everything from voice recognition and facial recognition to fingerprint scanning, retinal scans and even blood samples are all used for security and identity authentication.




VARIOUS TYPES OF BIOMETRIC INFORMATION ARE USED FREQUENTLY:

	FACIAL RECOGNITION: Airports in New York City and Atlanta are already using facial recognition technology for international flights and the technology is likely to expand to other areas of airports and other public forms of travel as well.
	EYE SCANS: The human retina and iris are used in many technology companies and secure government facilities as identity authentication for security purposes.
	HAND RECOGNITION: Full hand scanning is used in law enforcement, criminal background checks and security. Similar to fingerprints, the overall shape and minutiae of the hand can create a unique identifier.
	FINGERPRINT RECOGNITION: For decades, the fingerprint has been one of the primary identification tools of law enforcement. In recent years, fingerprint identification technology has become a popular tool for employers in the workplace.

FINGERPRINT TECHNOLOGY IN THE WORKPLACE

One of the most common problems with biometric privacy in the workplace involves the use of fingerprint technology. Many employers are requiring employees to compromise their biometric information privacy by introducing fingerprint technology in the workplace. While probably the oldest and most well-known of all biometric identifiers, fingerprints are also the most potentially dangerous for employees, as their use puts their entire identities and personal information at risk.

COMMON USES OF THIS TECHNOLOGY INCLUDE:

	TIME-KEEPING: Using fingerprint technology for time-keeping can help prevent cheating better than the traditional punch-card system. Fingerprint time-keeping can keep employees from punching in remotely for other employees who are skipping work.
	SECURITY: Rather than traditional locks and keys, some employers prefer fingerprint technology for its security and efficiency benefits.
	MONITORING: Biometric fingerprinting can also be used to monitor remote employees.

RISKS OF WORKPLACE FINGERPRINTING FOR EMPLOYEES

- **DISCRIMINATION:** Employers that have access to personal information available through fingerprint technology can discriminate against employees, based on the information gleaned through this technology.
- **INSURANCE FRAUD:** Similarly, if insurance companies can access personal information, they can use it to deny coverage based on health information and characteristics they see as risky.
- **CIVIL RIGHTS VIOLATIONS:** Once the personal identifying information of employees is stored and available to employers, it is not difficult to imagine situations in which the government could access and use that information illegally in violation of employees' civil rights.
- **IDENTITY THEFT:** Identity theft is by far the most significant risk to employees brought on by fingerprinting technology in the workplace.

BIOMETRIC IDENTITY THEFT

Everyone understands identity theft, generally. Accessing various forms of personal identifying information, an identity thief can use this information to access bank accounts, online assets and other aspects of a victim's financial portfolio.

The problem is much more complicated when it comes to biometric privacy. In cases of regular identity theft, the victim can change the information stolen. Credit card numbers, driver's license numbers and even Social Security numbers can be changed if they have been stolen.

Conversely, a victim's fingerprints or other biometric information cannot be changed once the identity theft is discovered. Conceivably, a biometric identity thief can change a victim's banking records and criminal records, get them placed on Homeland Security watch lists and generally destroy the victim's life.

This is an extremely important issue. Employees need to make sure their biometric privacy is protected in the workplace.



LEGAL PROTECTIONS FOR EMPLOYEES

With the risks involved with fingerprinting and other biometric identifiers in the workplace, what legal protections do employees have?

Unfortunately, not nearly enough.

There is no single unified federal law in place to protect consumers and employees from biometric privacy violations. The Health Insurance Portability and Accountability Act (HIPAA) privacy rules, the Federal Trade Commission (FTC) Act, Food and Drug Administration (FDA) regulations and other federal laws form a piecemeal legal landscape without a single unifying law providing a clear standard regarding the protection of biometric information privacy.ⁱⁱ

Legal protections in place at the state level are not much better. Illinois, Washington and Texas are the only states where it is illegal to identify individuals with images taken while they are in public, even without their consent.

In some ways, Illinois and California are two of the most important states leading the charge to provide consumers and employees with adequate legal protection for their biometric privacy rights.

Let's look at Illinois and California in more detail.





ILLINOIS' BIOMETRIC INFORMATION PRIVACY ACT (BIPA)

So far, Illinois has been the most progressive of all the states in its efforts to protect employee privacy rights from biometric privacy violations. It has the clearest and most detailed rules and regulations for employers using this technology, along with a private right of action for employees whose rights have been violated in this way.

Illinois passed its BIPA into law in 2008 to regulate employers' use of their employees' biometric information. The law covers only private employers; it does not extend to government employers in the state.

BEFORE OBTAINING OR TRANSFERRING ANY BIOMETRIC INFORMATION, PRIVATE ENTITIES IN ILLINOIS (INCLUDING EMPLOYERS) MUST:

- Develop a written policy, made available to the public, for biometric information retention and destruction, and employers must comply with the policies they've developed
- Inform subjects that their biometric privacy is being used, the purpose of the use and the details of retention and destruction schedules
- Obtain written consent as to biometric information collection, use, retention and destruction

Further, according to Illinois' BIPA, no private entity may disseminate anyone's biometric information without the subject's consent, except as required by law.ⁱⁱⁱ

BIPA



THE CALIFORNIA CONSUMER PRIVACY ACT (CCPA)

California has also been an important player in the protection of citizens' biometric privacy. The state's Consumer Privacy Act (CCPA) went into effect in 2018 to protect the personal information of California citizens.

California has legislative updates to CCPA slated for January 2020. Senate Bill 1121 is aimed at protecting employees against biometric privacy violations in the workplace.^{iv}

PRIVATE RIGHT OF ACTION IN ILLINOIS AND CALIFORNIA

While most states have either nothing on the books at all or legal schema that only provide statutory penalties for employers, but no private right of action, Illinois allows employees to bring claims directly against employers that misused or failed to protect their biometric privacy.

Recent amendments to the CCPA also include a private right of action.

This is an important distinction, meaning that individuals who have had their biometric privacy rights violated by employers or other entities can obtain compensation.

Further, in Illinois, a 2019 legal case, *Rosenbach v. Six Flags Entertainment Corp.*, established that a plaintiff does not even need to suffer specific damages to obtain compensation for violations of the BIPA.^v

Although Illinois case law is not binding everywhere, it certainly will be influential in other courts and legislatures exploring these issues. Even California, as a state intent on protecting biometric privacy, will likely take a similar approach.

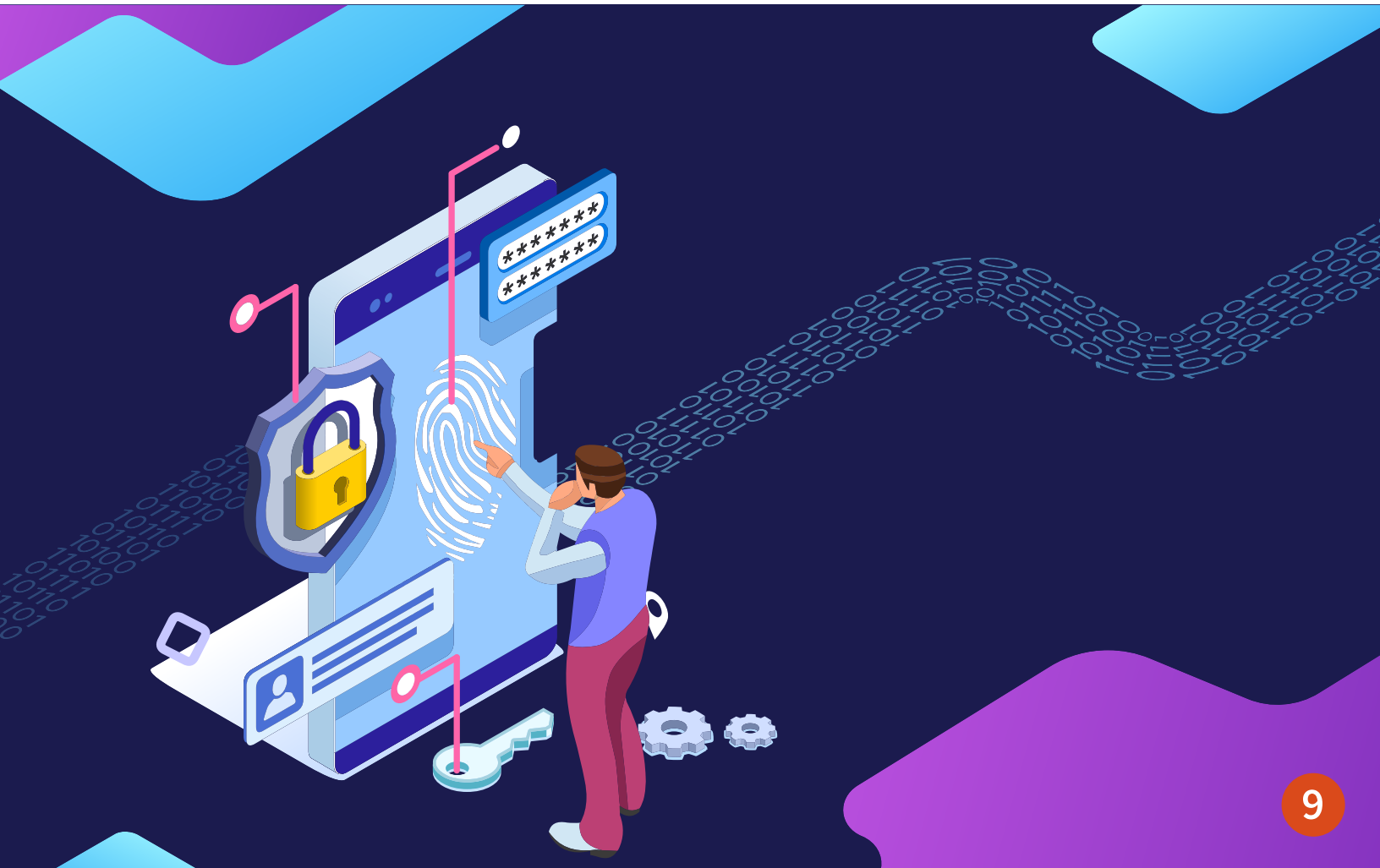
This means that if your employer violated your biometric privacy rights in Illinois and likely in California as well, you could obtain compensation even if you haven't been damaged personally by this violation.

HOW DO YOU KNOW IF YOUR RIGHTS HAVE BEEN VIOLATED AT WORK?

There are a couple of important things to look for to determine whether your employer (or another entity) has violated your rights:

- Have you been compelled to use fingerprint technology for identification, security or time-keeping?
- Did your employer inform you of its policies regarding the gathering, retention, dissemination and destruction of your fingerprint or other biometric information?
- Did your employer obtain your written consent for these activities?

Simply put: If your employer forced you to use your fingerprint for any purpose without informing you of its policies and retaining your written consent, you probably have a claim.



WHAT SHOULD YOU DO IF YOU HAVE A CLAIM?

The first thing you should understand is that *you have rights*. Although there are strict, clear laws in place in Illinois and California, no employer is going to voluntarily compensate anyone whose rights it may have violated.

Exercising your right to biometric privacy will almost certainly require the filing of a lawsuit.

Due to the complicated legal and scientific nature of this area of law, it is critical that you do not try to

handle your case alone or work with inexperienced counsel. At the Law Offices of Todd M. Friedman, we are on the cutting edge of consumer and employee rights litigation and the protection of biometric privacy.

With offices in California and Illinois, our attorneys have been keeping close watch on all of the developing legal issues related to biometric privacy, and we would be happy to discuss your rights and options with you.





ABOUT ATTORNEY TODD M. FRIEDMAN

FOUNDING PARTNER - THE LAW OFFICES OF TODD M. FRIEDMAN, P.C.
SUPER LAWYERS, 2016-2019

Many lawyers use the David-versus-Goliath metaphor to describe their practice. In the consumer protection field, that analogy is perhaps more apt than anywhere else. Standing up for consumers often requires battling large, powerful companies on a nationwide scale. As a champion for the underdog, I have successfully done just that.

I've built my career on protecting the rights of everyday people against unscrupulous businesses — particularly those that violate state privacy laws and federal laws, such as the Fair Debt Collection Practices Act and the Telephone Consumer Protection Act. Through consumer protection claims, including complex class actions on a nationwide scale, I have held companies accountable while securing compensation for those who have been wronged.

A prominent focus of my practice is the California Invasion of Privacy Act. As one of the first attorneys to successfully certify a class under section 632.7, I'm very familiar with the nuances and challenges of this niche area. I currently represent a class of consumers in a large-scale case against a debt collection company that illegally recorded cellphone calls with hundreds of debtors across California.

SUPER LAWYERS • 2016-2019

Super Lawyers is a patented rating service of outstanding lawyers who have attained a high degree of peer recognition and professional achievement. This exclusive honor is awarded to only the top 5 percent of attorneys per state.

Call our firm: **877-619-8966** | Visit our site: www.toddflaw.com

Share this white paper:    

The content of this paper is provided for informational purposes only and does not constitute legal advice.

© 2019 Law Offices of Todd M. Friedman, P.C.. All rights reserved. Design and editorial services by FindLaw, part of Thomson Reuters.



SOURCE INFORMATION

- i <https://www.gemalto.com/govt/inspired/biometrics>
- ii <https://www.gemalto.com/govt/biometrics/biometric-data>
- iii 740 ILCS 14 Biometric Information Privacy Act.
<http://www.ilga.gov/legislation/ilcs/ilcs3.asp?ActID=3004&ChapterID=57>
- iv https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180SB1121
- v Rosenbach v. Six Flags Entertainment Corp., 2019 IL 123186 (Jan. 25, 2019)
<http://www.illinoiscourts.gov/Opinions/SupremeCourt/2019/123186.pdf>

YOUR FINGERPRINTS, YOUR IDENTITY, YOUR PRIVACY

PROTECTING YOURSELF
IN THE WORKPLACE



A White Paper
Presented By

TMF LAW OFFICES OF
TODD M. FRIEDMAN, P.C.