

Employee Privacy Rights on the Ascendancy in Illinois

The Illinois Supreme Court's recent decision in [Rosenbach v. Six Flags Entertainment Corp.](#) holds two lessons for Illinois employers. First, Illinois employers must scrupulously comply with the [Illinois Biometric Information Privacy Act](#) ("Act"). No quarter will be given by class action attorneys if Illinois employers do not strictly comply with the Act. Second, Illinois employers must take the digital privacy rights of their employees seriously. Employers must do everything in their power to prevent data theft and identity theft that might otherwise hurt their employees.

1. Illinois' Biometric Privacy Act and the Holding in Rosenbach

Since 2008, the Act in Illinois imposes numerous restrictions on employers as to how they collect, retain, disclose and destroy biometric data. Common biometric identifiers are retina or iris scans, fingerprints, voiceprints, scans of hand or face geometry, or biometric information. As we discussed in a prior [article](#) on the Act, many employers use biometric data in connection with their timekeeping devices for their non-exempt employees.

In *Rosenbach*, the Illinois Supreme Court was asked to interpret the Act for the first time and asked to determine whether a mere "technical violation" under the Act will entitle an individual to recover damages under the Act. The *Rosenbach* decision was not close. The Court held without dissent that mere "technical violations" under the Act are actionable. The Court's decision was based on a plain reading of the statute, a historical definition of what it means to be an "aggrieved" party, and the Illinois Assembly's stated risks of the use of biometric information.

2. How Should Employers Handle Biometric Information Going Forward

In 2016 we identified the risks associated with the use of biometric information and recommended, perhaps naively, that employers not use it at all until the Illinois legislature changed the Act. The Illinois legislature

is not going to change the Act any time soon and Governor Pritzker probably would not agree to such a change in any event. ([Wednesday Evening Word No. 28](#)).

Since biometric information is not going away, Illinois employers must educate themselves on the fine points of the Act. Employers must ensure that: (1) they properly inform their employees *in writing* of the biometric information they are collecting, capturing or storing; (2) inform employees of the specific purpose for the collection of biometric data and how long the employer is keeping the data; and (3) obtain a written release before collecting the information.

3. Employers Must Start Thinking More Broadly about Employee Privacy Issues

The larger issue that *Rosenbach* raises is employee privacy rights more generally, particularly in the digital sphere. In the past, private sector employers in Illinois were not constrained by the U.S. or Illinois constitutions and they could be confident that employee privacy rights in the workplace were minimal. The growing push for comprehensive [data privacy rights](#) at the federal level will regulate employer conduct. Concrete steps to [protect employees' digital information](#) must be a high priority for employers.

Ross I. Molho
Clingen Callow & McLean, LLC
2300 Cabot Drive, Suite 500
Lisle, Illinois 60532
www.ccmlawyer.com
(630) 871-2614

The author, publisher, and distributor of this CCM Alert is not rendering legal or other professional advice or opinions on specific facts or matters. Under applicable rules of professional conduct, this communication may constitute Attorney Advertising.

© 2019 Clingen Callow & McLean, LLC. All rights reserved.

ccmlawyer.com