

Global Use and Regulation of Social Media

Prepared by:
Ambrose V. McCall
Hinshaw & Culbertson LLP



LORMAN[®]

Published on www.lorman.com - September 2021

Global Use and Regulation of Social Media, ©2021 Lorman Education Services. All Rights Reserved.



Lorman Education Services is a leading provider of online professional learning, serving individuals and teams seeking training and CE credits. Whether you're looking for professional continuing education or an enterprise-wide learning and development solution, you will find what you need in Lorman's growing library of resources.

Lorman helps professionals meet their needs with more than 100 live training sessions each month and a growing collection of over 13,000 ondemand courses and resources developed by noted industry experts and professionals.

Learn more about Lorman's individual programs, economical All-Access Pass, and Enterprise Packages:

www.lorman.com

Global Use and Regulation of Social Media

Prospective employees, however, come from many locations around the globe. Therefore, prospective employers must keep in mind that other countries or jurisdictions may have different policies regarding the use of personal social media webpages by prospective employers. For example, on June 12, 2009, the European Union adopted a May 2009 opinion regarding online social networking known as Article 29, Data Protection Working Party. In the adopted opinion, the European Union noted that the secure processing of information constitutes a key element of trust placed by users in social media network sites which the EU describes as social network services (SNS). *Id.* at Section 3.2 Security and Default Privacy Settings, p. 7. The EU policy notes that privacy settings prove crucial with respect to the access of a user's personal data detailed in a profile. Without any restrictions to accessing such data, third parties may access, use, or link all types of intimate details regarding users as another member of the same SNS or through search engines. *Id.* In light of the majority of users signing up at SNS sites without making any changes to the default privacy settings, the EU asserts that SNS should offer "privacy-friendly default settings" which allow users to easily restrict access to their data by third parties. If the restricted access is opted for by the user, the EU asserts that the restricted access profiles "should not be discoverable by internal search engines, including the facility to search by parameters such as age or location." *Id.* As a result, while the EU has not yet installed a double pane privacy window around social media sites, it does appear that the trend in the European Union is moving toward requiring greater privacy protections for users of social media sites. More recent pronouncements by the European Union only further underscore its stated intent to provide persons with greater privacy protections. Article 29 Working Party.

In 2018, the EU adopted the General Data Protection Regulation (GDPR). That regulation applies to US or international companies with employees located in the EU. That EU law imposes numerous regulations on such business outside the scope of this discussion.

One must also note that all potential claims of invasion of privacy necessarily rely on a showing by the claimant that he or she possesses a reasonable expectation of privacy. *See City of Ontario v. Quon*, 130 S.Ct. 2619, 2630 (2010) ("Cell phone and text message communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification. That might strengthen the case for an expectation of privacy. On the other hand, the ubiquity of those devices has made them generally affordable, so one could counter that employees who need cell phones or similar devices for personal matters can purchase and pay for their own. And employer

policies concerning communications will of course shape the reasonable expectations of their employees, especially to the extent that such policies are clearly communicated."). Subsequent case law that construes the discussion in *Quon* highlights the potential for a workplace search to be found unreasonable, if it does not violate, for example, the constitutional rights of an employee. See *Cunningham v. N.Y. State Dep't of Labor*, 21 N.Y.3d 515, 997 N.E.2d 468, 470, 473, (N.Y. Ct.App.2013) ("The State of New York, suspecting that one of its employees was submitting false time reports, attached a global positioning system (GPS) device to the employee's car.")("We hold the search did not require a warrant, but that on the facts of this case it was unreasonable.")("Where an employer conducts a GPS search without making a reasonable effort to avoid tracking an employee outside of business hours, the search as a whole must be considered unreasonable. That conclusion concededly requires suppression of the GPS evidence here;")(not suppressing E-Z Pass record evidence); *compare with Carniol v. N.Y.C. Taxi & Limousine Comm'n*, 42 Misc.3d 199, 975 N.Y.S.2d 842, 848-50 (N.Y. Sup. Ct. 2013)("Here, the TTS system was installed with the knowledge of the taxicab owners and all taxicab drivers are required to follow TLC regulations which mandate the use of the TTS system.")("However, even if petitioner could show that he has a legitimate expectation of privacy in trip data gathered by the GPS device, which he cannot, his fourth amendment claim of privacy would be outweighed by the legitimate governmental interests articulated by the TLC")("In this case, Caniol's privacy interest in the trip data generated by the GPS device is minimal and the government's intrusion is also minimal.")([I]t does not collect data regarding Caniol's whereabouts when he is off-duty.")("Here, the TTS equipment placed in each New York City taxicab electronically tracks location, trip and fare information only while the driver is on duty. The purpose of the GPS is to gather information pertaining to the taxicab business. It is not used to collect personal information about the drivers.").

The same privacy concerns, when discussed within the context of government employment and associated constitutional protections, even limits the scope of drug testing programs that lack a required job category safety analysis or individual basis for suspicion. *Am. Fed'n of State, County & Mun. Employees Counsel 79 v. Scott*, 717 F.3d 851, 866, 879-80 (11th Cir. 2013)("The basic question we are required to answer when confronted with a drug-testing policy is whether the search is reasonable.")("None of the State's proffered rationales warrant summary judgment in the State's favor concerning all job categories and all employees covered by the EO.")("[T]he State has failed to demonstrate that all 85,000 state employees somehow have diminished privacy rights. Moreover, it has failed to provide a compelling or important reason for testing; indeed, it has offered only general and weak justifications regarding workplace efficiency and the possible –

not 'substantial and real,' (cite omitted) – risks to safety that any state employee my pose.").

Social Media Profiles and Anti-Discrimination Laws

Employers may not use social media profile data or any other information in hiring decisions in a manner that violates anti-discrimination laws, such as federal laws prohibiting discriminatory hiring decisions based on the race, color, religion, sex, national origin, or disability of the applicant. See, Title VII of the Civil Rights Act of 1964, 42 USC §§2000e to 2000e-17; Americans with Disabilities Act, 42 USC §§12111-12117. Federal law also bars discriminatory hiring decisions based on applicants' ages of 40 or greater. Age Discrimination in Employment Act, 29 USC §§621-33a. Illinois law expands even farther in barring employers from discriminating against applicants because of their race, color, religion, sex, national origin, ancestry, age, marital status, physical or mental disability, military status, sexual orientation, or unfavorable discharge from military service in connection with employment, real estate transactions, access to financial credit and the availability of public accommodations. 775 ILCS 5/1-102(A). As of January 1, 2010, the cited Illinois statutory provision also bars discrimination against applicants due to their order of protection status. (Public Act 096-0447 amending 775 ILCS 5/1-102(A)). The amending language defines "order of protection status" as meaning "a person's status as being a person protected under an order of protection issued pursuant to the Illinois Domestic Violence Act of 1986 or an order of protection issued by a court of another state." (Public Act 096-0447 amending 775 ILCS 5/1-103 so as to insert new statutory provision (K-5) effective January 1, 2010, and again specifically inserting "order of protection status" as within category of unlawful discrimination as designated in Public Act 096-0447 amending 775 ILCS 5/1-103(Q)).

What this quick statutory review indicates that privacy interests of prospective applicants in their social media site data currently exists, if even to a limited extent, under many state laws. Therefore, employers should monitor regulatory advances undertaken by state and federal Departments of Labor, among others, as well as standards implemented in the countries or jurisdictions outside of the United States from whom employers may recruit prospective employees. In addition, however, should employers consider using social media site data to screen applicants, care should be taken to avoid using any social media site data in an unlawful discriminatory manner, or as the sole basis for a hiring decision.

One may currently analogize to employers who check the criminal records of applicants. While such practices are not illegal, to the extent that any hiring or employment decisions are consistent with "business necessity" and do not

negatively impact a category of applicants in a disparate manner, other concerns may exist. For example, 40 or more states have prohibited the use of arrest records for use in employment decision making processes. Steven F. Befort, "Pre-Employment Screening and Investigation: Navigating Between a Rock and a Hard Place," 14 Hofstra Lab. L. J. 365, 404-05 (1997) (rationalizing that "conviction records are more reliable... because the criminal justice system has established that misconduct actually occurred"). As a result, a majority of states restrict or prohibit the use of arrest records by employers over concerns that the lack of established guilt will be used in a potentially discriminatory manner. Rochelle B. Ecker, Comment, To Catch a Thief: The Private Employer's Guide to Getting and Keeping an Honest Employee, 63 U.N.K.C.L. Rev. 251, 255-56 (1994). Moreover, employers have also seen growth in "ban the box" laws, which typically compel an employer to first consider the qualifications of an applicant before later having a background check conducted on an applicant. (State laws placing limits and/or disclosure obligations on use of criminal conviction data by public employers – Ariz. Rev. Stat. §31-51i; Conn. Gen. State. §46a-80(c); Fla. Stat. §112.011; Ky. Rev. Stat. §335 B. .010(4), .020, .070; La. Rev. Stat. §37:2950; Minn. Stat. §364.03; Neb. LB907; N.M. Stat. §§28-2-3, 28-2-4, 28-2-5, and 28-2-6; Wash. Rev. Code §§9.96A.020, 9.96A.060, and 9.96A.030. In general, the cited laws require some information that explains a connection between the conviction and the applied for job, in order for the conviction to be used as a disqualifying factor, but each state law, creates its own decision true analysis that compels a review of the circumstances of each applicant, the conviction data, and the specific duties of each job. The same concerns apply to the state laws regulating the use of conviction data for both private and public employers. Haw. Rev. Stat. §378-2.5(a); Ill. HB570-1, 820 ILCS 75/1 et seq., Kan. Stat. Ann. §22-4710(E); New Jersey P.L. 2014, c.32; N.Y. Exec. Law §296(15), (16); N.Y. Correct. Law §§750-754; 18 Pa. Cons. Stat. §§9124-99125; Wis. Stat. §111.335.

In a somewhat similar fashion, unless otherwise authorized by law, under Illinois law, it is a civil rights violation for any employer, employment agency or labor organization to inquire into or use the fact of an arrest or criminal history record information ordered expunged, sealed or impounded under Section 5 of the Criminal Identification Act, as grounds to not hire or segregate an applicant with respect to recruitment, hiring, promotion, renewal of employment, selection for training or apprenticeship, discharge, discipline, tenure or terms, privilege or conditions of employment. 775 ILCS 5/2-103(A). The cited section exempts state agencies, local governmental units or school districts, and private organizations from requesting or utilizing sealed felony conviction information obtained from the Department of State Police under Section 3 of the Criminal Identification Act or under other federal or state laws or regulations that compel the performance of criminal background checks in evaluating the character or qualifications of

prospective employees or employees. *Id.* Moreover, one must also note that the cited statutory prohibition is not to be construed as barring an employer, employment agency or labor organization from obtaining or using other information which indicates that an applicant or employee actually engaged in the conduct for which he or she was arrested. 775 ILCS 5/2-103(B).

An additional pre-employment screening concern may arise with the Fair Credit Reporting Act. The FCRA prohibits employers from procuring credit reports on job applicants without previously receiving the consent of the individual applicant. 15 USC §§1681-1681t. For example, the Fair Credit Reporting Act compels an employer to “clearly and accurately” inform applicants in writing that they will be the subject of a consumer credit report that a consumer reporting agency will prepare. 15 USC §1681d. Moreover, if the credit report is used in making an unfavorable hiring decision, the applicant must receive notice of such use of the credit report. 15 USC §1681m. In addition, employers may not base their hiring decision solely on the results detailed in the credit report and may incur liability if their decisions based on such reports impact a protected class in a disparate manner. *Id.* See also 11 USC §525(b) (Bankruptcy Act’s prohibition against private employers terminating an employee solely because he is a debtor or because he is bankrupt).

Do Common Law Privacy Claims Apply?

Still, the Illinois Supreme Court explained how the common law tort of intrusion upon a person's seclusion may lead to a former employer sustaining liability in tort for compensatory and punitive damages. In *Lawler v. North American Corp. of Illinois*, 2012 IL 112530 (Ill. 2012), the former employer hired detectives who impersonated as the plaintiff in order to obtain her phone records. The Illinois Supreme Court cited and quoted from the Restatement (Second) of Torts as follows:

Section 625B of the Restatement (Second) of Torts provides: 'One who intentionally intrudes, physically or otherwise, upon the seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy if the intrusion would be highly offensive to a reasonable person.' Restatement (Second) of Torts §652B (1977). For purposes of illustration relevant to the facts in this case, comment b to Section 652B of the Restatement provides, in pertinent part:

b. The invasion may be ... by some other form of investigation or examination into his private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private

bank account or compelling him by a forged court order to permit an inspection of his personal documents. The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the *** information outlined. Restatement (Second) of Torts §652B.

Lawlor, 2012 IL 112530 at ¶33. The *Lawlor* court affirmed plaintiff's compensatory damage award of \$65,000, but further reduced the jury award of \$1.75 million in punitive damages to \$65,000. *Id.* at ¶¶1, 76.

The Iowa Supreme Court also applied the intrusion upon seclusion analysis when finding that the disputed actions by an employer who had secretly installed surveillance equipment in a workplace bathroom was subject to a trial on the merits.

"Importantly, the cause of action for invasion of privacy imposes liability based on a particular method of obtaining information, not the content of the information obtained, or even the use put to the information by the intruder following the intrusion."

"Thus, a belief by a plaintiff that a person invaded his or her privacy by placing an apparent recording device in a private area does not establish an intrusion if the device was not capable of being configured or operated to transmit or record in any conceivable way. Accordingly, proof the equipment is functional is an ingredient in the inquiry. Indeed, the very purpose of the tort is to protect the opening up of a private place where the plaintiff seeks seclusion. (cite omitted). If the fact finder finds from the evidence that the device could not have intruded into the privacy of the plaintiff in any manner, the tort of invasion of privacy has not been committed. Yet, if the fact finder finds from the evidence that the device could have intruded into the privacy of the plaintiff, the element of intrusion is satisfied."

"An electronic invasion occurs under the intrusion or solitude or seclusion component of the tort of invasion of privacy when the plaintiff establishes by a preponderance of evidence that the electronic device or equipment used by a defendant could have invaded privacy in some way."

Koeppel v. Speirs, 808 N.W.2d 177, 180, 184-85 (Iowa 2011). Moreover, an employer who intentionally places an inoperable camera, recording device, or other piece of electronic or digital monitoring equipment into a private area of its

employees may become the subject of a common law tort claim of intentional infliction of emotional distress. *Koeppel*, at n.2.

Illinois Statutory Protections

Illinois enacted the Right of Publicity Act in 1999. 765 ILCS 1075/1. The Right of Publicity Act recognizes an individual's "right to control and to choose whether and how to use [that] individual's identity for commercial purposes ..." 765 ILCS 1075/10. The Act defines "Identity" to include personal characteristics that include but are "not limited to (i) name, (ii) signature, (iii) photograph, (iv) image, (v) likeness, or (vi) voice." 765 ILCS 1075/5 (Definition of "Identity"). The Act covers live and deceased persons, whether or not their identity was "used for a commercial purpose during the individual's lifetime." 765 ILCS 1075/5 (definition of "Individual"). The Act broadly defines "Name" to mean "the actual name or other name by which an individual is known that is intended to identify that individual." 765 ILCS 1075/5 (definition of "Name"). The Act also characterizes a wide range of media and materials as part of a protected "Work of Fine Art." 765 ILCS 1075/5 (definition of "Work of Fine Art.").

Not surprisingly, the Act broadly defines "Commercial Purpose" to include publicly holding out or using a person's "Identity" for fundraising purposes among the covered activities, in addition to offering for sale or selling products, merchandize, goods, and services, and advertising or promoting such offers or sales. 765 ILCS 1075/5 (definition of "Commercial Purpose").

The Act explains that the individual's right of publicity is freely transferable by a "written transfer," as well as by way of a will or intestate succession. 765 ILCS 1075/15. The individual, or his or her authorized representative, or written transferee, or person who possesses such rights after the individual's death may pursue remedies that the Act provides. 765 ILCS 1075/20(a). A deceased individual's rights terminate when there is no written transferee and no living spouse, parents, children, or grandchildren. 765 ILCS 1075/25.

The result is that one may not use an individual's identity for commercial purposes without having the written consent from the appropriate persons or their authorized representatives. 765 ILCS 1075/30(a). For an individual who dies after the January 1, 1999, effective date of the Act, that identity may not be used for 50 years after the date of death in the absence of written consent. 765 ILCS 107/30(b).

The Act does not apply to the use of an individual's identity in a work of fine art, or for non-commercial news purposes, or when identifying the individual as the author of a "work or program or the performer in a particular performance." 765 ILCS

1075/35(b)(1)-(3). Promotional materials, ads, or commercial announcements related to such uses also fall outside the scope of the Act. 765 ILCS 1075/35(b)(4).

Special circumstances and conditions apply to professional photographers which allow them to use an individual's identity, with "photographs, videotapes, and images...", "to exhibit in or about the professional photographer's place of business or portfolio, specimens of the professional photographer's work, unless the exhibition is continued by the professional photographer after written notice objecting to the exhibition has been given by the individual portrayed." 765 ILCS 1075/35(b)(5).

A successful plaintiff who establishes a violation of the Act may recover the greater dollar sum of:

"(1) actual damages, profits derived from the unauthorized use, or both; or

(2) \$1,000."

765 ILCS 1075/40(a)(1),(2). Punitive damages are available to be awarded against a person who willfully violates the limitations the Act imposes on the use of an individual's identity. 765 ILCS 1075/40(b). A successful plaintiff may also obtain injunctive relief against a violator and recover attorney's fees and costs. 765 ILCS 1075/50; 765 ILCS 1075/55.

The plaintiff bears the burden of proving damages or gross revenues associated with the unauthorized use. 765 ILCS 1075/45(a). Defendants are "required to prove properly deductible expenses." 765 ILCS 1075/45(b). The Act supplements, and does not replace, any common law rights an individual may also possess. 765 ILCS 1075/60.

Toney v. L'Oréal USA, Inc., 406 F.3d 905, 910 (7th Cir. 2005).

The court discussed the following analysis in response to a plaintiff's claim that her photograph was used to advertise a hair product that Johnson Products Company marketed. Plaintiff claimed that she consented to a limited time use of her photograph, but not the later use of her photograph by a successor company which she claims was done without her permission. Plaintiff sued and claimed that the successor company had violated her right of publicity. The trial court had dismissed her claim upon finding that federal copyright law preempted her cause of action. The U.S. Court of Appeals reversed.

"Clearly the defendants used Toney's likeness without her consent for their commercial advantage. The fact that the photograph itself could be

copyrighted, and that defendants own the copyright to the photograph that was used, is irrelevant to the IRPA claim. The basis of a right of publicity claim concerns the message – whether the plaintiff endorses or appears to endorse the product in question. One can imagine many scenarios where the use of a photograph without consent, in apparent endorsement of any number of products, could cause great harm to the person photographed. The fact that Toney consented to the use of her photograph originally does not change this analysis. The defendants did not have her consent to continue to use the photograph, and therefore, they stripped Toney of her right to control the commercial value of her identity."

Brown v. Acmi Pop Div., 375 Ill.App.3d 276, 873 N.E.2d 954, 962 – 63 (1st Dist. 2007).

The Illinois Appellate Court later answered two certified questions regarding the extent of protections provided by the Illinois Right of Publicity Act. In sum, the Appellate Court found that the trial court had properly denied a motion to dismiss the plaintiffs' causes of action that relied on the Illinois Right of Publicity Act. The court also found that the U.S. Copyright Act does not preempt Illinois publicity and privacy claims.

"In light of the vast difference of opinion regarding the interpretation of the definition of what Corbis sells and the legal effect of such sales, we cannot say that the facts are undisputed that Corbis's display of the photos of James Brown on its Web site did not in some way constitute an improper commercial use under either the Illinois common law or the Publicity Act. We therefore cannot conclude that the trial court erred in denying Corbis's motion to dismiss.

Brown argues that the images of James Brown advertised for sale on Corbis's website do, in fact, constitute fixed work on the Internet in that the "licenses" result in a tangible photograph to the end-user. Brown distinguishes *Laws* [v. *Sony Music Entertainment, Inc.*, 448 F.3d 1134, 1136 (9th Cir. 2006)], noting that there, the plaintiff had contractually released control and copyright of her recording to Sony. By contrast, Brown never consented to any sale of his photographs and never possessed control of the copyright interest to release.

Under the circumstances, where it is possible that the photos as displayed on Corbis's Internet Web page can be interpreted as tangible, the Publicity Act as applied here would not preempt copyrights. As such, we answer the second question certified to this court in the negative."

Trannel v. Prairie Ridge Media, Inc., 2013 IL App (2d) 120725 at ¶¶25, 26, 987 N.E.2d 923, 931 (2nd Dist. 2013).

The Illinois Appellate Court held that one use of photograph of plaintiff was for a "news" purpose and therefore was not covered by the Illinois Right to Publicity Act. In contrast, the defendant's use of the same photograph for a second purpose, specifically as a cover page of a media kit, did violate the Illinois Right to Publicity Act.

"Contrary to defendant's argument, we believe that the two publications of the subject photograph were for entirely different purposes, one covered by the Act, one not. [...] In this respect, 'news' is broader than reporting on public affairs, that is, politics and public policy. The subject photograph appeared in the autumn 2009 issue of the magazine in connection with the announcement of the garden-contest winners. Reporting who won the contest was reporting a recent event and new information. Thus, the use of the subject photograph to accompany the article was for the purpose of 'news' and was exempted from the Act. Indeed, such types of events are regularly reported on the local nightly news broadcasts.

On the other hand, as we demonstrated above, the use of the subject photograph on the cover of the media kit was for commercial purposes, as defined by the Act. Consequently, defendant needed plaintiff's written consent to use the subject photograph on the media kit. Defendant contends that such consent can be found in the rules for the garden contest and in the emails plaintiff exchanged with members of defendant's staff. Nowhere in the rules is there any language that would advise a contest entrant that, by entering the contest, he or she agreed to the unlimited use of his or her likeness for commercial purposes. Nor do the emails establish such consent. Plaintiff's email served as her entry form. Defendant advised plaintiff by email that she was a finalist and would be contacted by Pendergrast. This email mentioned the photographer but did not reference any uses to be made of the photographs. The email in which defendant advised plaintiff that she was a winner contained the information that the autumn issue of the magazine was 'chock-full' of photos and details about the gardens. That email made no mention of the subject photograph or using it for purposes other than in connection with the article announcing the winners. Accordingly, we conclude that use of the subject photograph on the cover of the media kit without plaintiff's written consent violated section 30 of the Act."

The Biometric Information Privacy Act – 740 ILCS 14/1 et seq.

The Biometric Information Privacy Act, commonly known as “BIPA”, was enacted by the Illinois legislature in 2008. The stated intent of BIPA is help regulate “the collection, use, safeguarding, handling, storage, retention, and destruction of biometric identifiers and information.” *Id.* at §5(g). The Act defines the term “Biometric identifier” as including “a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry.” *Id.* at §10. The statutory definition of “Biometric information” encompasses “any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual.” *Id.*

The significance of BIPA is that through Section 15 it imposes on private entities a series of obligations that relate to and arise from the collection, retention, disclosure, and destruction of biometric identifiers and biometric information. Those obligation include:

- (i) obtaining the consent of individuals if the company plans to collect, store, or disclose their personal biometric identifiers;
- (ii) using a writing to inform the individuals of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used;
- (iii) timely destroying the biometric identifiers; and
- (iv) securely storing the biometric identifiers.

740 ILCS 14/15.

BIPA also supplies a private right of action that provides a prevailing party with remedies including the ability to recover liquidated damages of \$1,000 or actual damages if greater, for negligent violations of the Act. A plaintiff who establishes that a defendant intentionally or willfully violated the Act may recover liquidated damages of \$5,000 or actual damages if greater. The successful claimant can also recover attorney’s fees, costs, and expenses. 740 ILCS 14/20.

In 2019, the Illinois Supreme Court held that a BIPA plaintiff need to plead and prove that he or she sustained an actual concrete injury in order to proceed with a claim under the Act. *Rosenbach v. Six Flags Entm’t Corp.*, 2019 IL 123186, ¶¶38-40, 129 N.E.3d 1197, 1207 (2019) (“Contrary to the appellate court’s view, an individual need not allege some actual injury or adverse effect, beyond violation of his or her rights under the Act, in order to qualify as an “aggrieved” person and be entitled to seek liquidated damages and injunctive relief pursuant to the Act.”).

After issuance of the *Rosenbach* opinion, many class action complaint have been filed that cite to or rely on BIPA.

But in an opinion that found insurance coverage to exist for an entity facing a BIPA claim, the Appellate Court of Illinois interpreted an insurance policy's coverage for defamation claims to extend to and include BIPA claims under the policy's definition of "personal injury" which included the "oral or written publication of material that violates a person's right of privacy." *W. Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc.*, 2020 IL App (1st) 191834, ¶¶25-38.

Moreover, the Illinois Appellate Court also read an arbitration agreement that covered wage and hour claims as not including employee BIPA claims. *Liu v. Four Seasons Hotel, Ltd.*, 2019 IL App (1st) 182645, ¶30, 138 N.E.2d 201 (1st Dist. 2019)(In short, the Act is a privacy rights law that applies inside and outside the workplace.)(“Simply because an employer opts to use biometric data, like fingerprints, for timekeeping purposes does not transform a complaint into a wages or hours claim.”).

The material appearing in this website is for informational purposes only and is not legal advice. Transmission of this information is not intended to create, and receipt does not constitute, an attorney-client relationship. The information provided herein is intended only as general information which may or may not reflect the most current developments. Although these materials may be prepared by professionals, they should not be used as a substitute for professional services. If legal or other professional advice is required, the services of a professional should be sought.

The opinions or viewpoints expressed herein do not necessarily reflect those of Lorman Education Services. All materials and content were prepared by persons and/or entities other than Lorman Education Services, and said other persons and/or entities are solely responsible for their content.

Any links to other websites are not intended to be referrals or endorsements of these sites. The links provided are maintained by the respective organizations, and they are solely responsible for the content of their own sites.