No. 123186

IN THE SUPREME COURT OF ILLINOIS

STACY ROSENBACH, as Mother and Next Friend of Alexander Rosenbach, individually and as the representative of a class of similarly situated persons,

Plaintiff-Appellant,

v.

SIX FLAGS ENTERTAINMENT CORPORATION and GREAT AMERICA LLC,

Defendants-Appellees.

On Appeal from the Appellate Court of Illinois, Second District, No. 2-17-0317
There on Appeal from the Circuit Court of Lake County, Illinois, No. 2006 CH 13,
The Honorable Luis A. Berrones, Judge Presiding

BRIEF OF *AMICI CURIAE* THE RESTAURANT LAW CENTER AND ILLINOIS RESTAURANT ASSOCIATION IN SUPPORT OF DEFENDANTS-APPELLEES

Melissa A. Siebert
ARDC # 6210154
Bonnie Keane DelGobbo
ARDC #6309394
BAKER HOSTETLER LLP
191 North Wacker Drive, Suite 3100
Chicago, IL 60606
(312) 416-6200
msiebert@bakerlaw.com
bdelgobbo@bakerlaw.com

Angelo I. Amador
Restaurant Law Center
2055 L Street, NW
Suite 700
Washington, DC 20036
(202) 492-5037
aamador@restaurant.org

Attorneys for Amici Curiae

E-FILED
9/18/2018 10:28 AM
Carolyn Taft Grosboll
SUPREME COURT CLERK

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

POINTS AND AUTHORITIES

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

STATEMENT OF INTEREST

Since last August, approximately 120 class actions have been filed in Illinois state courts under the Biometric Information Privacy Act ("BIPA"). The vast majority of these lawsuits (88%) challenge employees' daily and *knowing* use of finger, hand, or facial scanning time-clocks to clock in and out of work to get paid. A significant number of restaurant and foodservice employers have been named as defendants in these BIPA class actions (21% of all BIPA cases[1]), due to their use of timekeeping and/or standard point of sale ("POS") systems, which scan employees' fingertips, hands, or facial features to provide secure access to timekeeping, customer orders, and credit card processing. The foodservice industry employee-plaintiffs claim that they are "aggrieved" under BIPA because they did not also receive advance written notice and agree in writing to that which they have known all along—that finger, hand, or facial scans are being used for timekeeping and customer order processing—activities they consent to on a daily basis.

Overturning *Rosenbach* on the bases proposed by Plaintiff and her *amici* could have a devastating impact on thousands of Illinois employers who have used scan-based timekeeping openly in good faith to comply with state and federal work hour tracking requirements. This group includes the significant number of restaurant and food service employees against whom scan-based timekeeping claims currently are pending. BIPA limits a cause of action to a "person aggrieved." Restaurant and other foodservice industry employees are not "aggrieved" because each day they show up to their places of employment and knowingly and willingly consent to the use of their finger, hand, or facial

[1] This figure includes restaurants, food manufacturers, food suppliers, and food distributors, all of whom fall within the foodservice industry. The statistics in this paragraph are based on BIPA filings through August 2018.

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

scans to ensure they get paid for their work. Yet restaurant and foodservice industry employee-plaintiffs want to argue that employers have virtually automatic liability if certain procedural requirements under BIPA are not followed.

The foodservice industry is the largest private sector employer in Illinois. In 2018, it is projected to employ 577,000 Illinois residents, and to generate over $25.2 billion in annual, taxable sales. *See* https://www.illinoisrestaurants.org/page/AboutUs (last visited Aug. 23, 2018). In the United States, the foodservice industry is comprised of over one million restaurants and other foodservice outlets employing almost 15 million people—approximately 10 percent of the U.S. workforce. Nationwide, restaurants and other foodservice providers are the second-largest private-sector employer.

Amicus Restaurant Law Center ("Law Center") is a public policy organization affiliated with the National Restaurant Association, the largest foodservice trade association in the world. *Amicus* the Illinois Restaurant Association provides valuable business services, including advocacy, to the Illinois foodservice industry. The Law Center provides courts with the industry's perspective on legal issues significantly impacting it. Specifically, the Law Center highlights the potential industry-wide consequences of pending cases such as this one, through *amicus* briefs on behalf of the industry. Brief of Restaurant Law Center et al. in *Epic Systems Corp. v. Lewis*, Nos. 16-285, 16-300 & 16-307 (U.S.) (brief in support of appellants from the Seventh, Ninth and Fifth Circuits regarding employers' ability to enforce class action waivers/individual arbitration agreements); Brief of Restaurant Law Center et al. in *Haynes v. Outback Steakhouse of Florida, LLC*, Appeal No. 17-13776 (11th Cir.) (brief in support of Outback Steakhouse opposing "copycat" lawsuits during website remediation period, following

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

settlement/judgement on Americans With Disabilities Act (ADA) website access claims); Brief of Restaurant Law Center et al. in *Winn-Dixie Stores, Inc. v. Juan Carlos Gil*, Appeal No. 17-13467 (11th Cir.) (brief in support of Winn-Dixie asserting that the ADA does not apply to websites, and that requiring compliance with unofficial guidelines violates due process and administrative law principles); *Guillermo Robles v. Domino's Pizza LLC*, Appeal No. 17-55504 (9th Cir.) (same).

The Law Center has a substantial interest in this case because overturning *Rosenbach* could have devastating consequences for the foodservice industry, which employs hundreds of thousands of Illinoisans—more than any other industry in Illinois. *Rosenbach* arose in the consumer context, so Plaintiff and her *amici* focus on BIPA's application in the consumer setting. However, approximately 88% of BIPA cases to date have arisen in the employment setting. This Court's decision will have a significant impact on Illinois employers, and on restaurants and foodservice employers in particular, as over one-fifth of the pending BIPA cases involve this industry. Allowing purely procedural violations of BIPA to render a person "aggrieved" could subject employers to potentially ruinous liability claims; employee-plaintiffs seek liquidated damages of $1,000 or $5,000 per BIPA "violation"—a term that is not defined in BIPA and which many BIPA plaintiffs are contending is payable for each separate time an employee clocks in or out of work or uses a POS system. This brief will assist the Court by addressing the unique implications of Plaintiff's proposed interpretation of BIPA in the employment context.

INTRODUCTION

BIPA should not apply in the employment timekeeping or POS context because employees knowingly and willingly use their finger, hand, or face to clock in and out of

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

work or operate POS systems every workday. Neither the text of BIPA nor Illinois case law support creating a privacy right in the finger, hand, and facial scans related to employer timekeeping or POS systems. Reading BIPA to impose penalties on employers for collecting, storing, and using such finger, hand, and facial scans with employees' knowledge and consent, has the potential to devastate the largest private sector employer in Illinois, and would violate employers' due process rights.

ARGUMENT

I. EMPLOYEES WHO KNOWINGLY AND WILLINGLY USE FINGER, HAND, OR FACIAL SCANS FOR TIMEKEEPING AND POS PURPOSES ARE NOT "AGGRIEVED."

BIPA provides a private right of action only to a "person *aggrieved* by a violation of this Act...." 740 ILCS 14/20 (emphasis added). The *Rosenbach* appellate opinion aptly noted that alleging a violation of BIPA is not the same as alleging that one is "aggrieved" by a violation, as "aggrieved" requires actual harm.

A significant common thread has emerged from cases interpreting BIPA—knowing and consensual conduct prevents one from meeting BIPA's actual harm requirements. In *McCollough v. Smarte Carte, Inc.*, No. 16 C 03777, 2016 WL 4077108, at *3 (N.D. Ill. Aug. 1, 2016), the court dismissed BIPA claims where the plaintiff alleged the defendant "violated BIPA by failing to obtain advance consent and inform her that it would retain her fingerprint data and for what period of time," but did "not allege any harm that resulted from the violation." That case involved a locker storage system that used finger scans. The court noted "[plaintiff] undoubtedly understood when she first used the system that her fingerprint data would have to be retained until she retrieved her belongings from the locker." Even if the defendant "did indeed retain the fingerprint data beyond the rental

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

period, this Court finds it difficult to imagine, without more, how this retention could work a concrete harm." *Id.* at *3-4.

The court in *Santana v. Take-Two Interactive Software, Inc.*, 717 F. App'x 12 (2d Cir. 2017) also dismissed BIPA claims where, despite asserted technical violations of BIPA's procedural requirements, it was clear the plaintiffs knowingly provided their biometric information to the defendant. *Santana* involved a computer game where players could scan their face to create a lookalike avatar. *Id.* at 13-14. The court reasoned plaintiffs could not allege any injury-in-fact under BIPA based on lack of written authorization because "[n]o reasonable person...would believe that the MyPlayer feature was conducting anything other than" a face scan when players "had to place their faces within 6 to 12 inches of the camera, slowly turn their heads to the left and to the right, and do so for approximately 15 minutes." *Id.* at 15-16. The *Santana* court also rejected an injury premised on lack of BIPA notice because "plaintiffs have not shown that this violation, if true, presents a material risk that their biometric data will be misused or disclosed." *Id.* at 16.

In the employment context, an even more compelling factual landscape in which employees willingly clock in and out of work each day, courts have held that employees cannot bring BIPA claims based on employers' use of a time-clock that allegedly uses biometric data, because an employee's use of the time-clock is necessarily knowing and consensual. For example, in *Howe v. Speedway LLC*, No. 17-CV-07303, 2018 WL 2445541 (N.D. Ill. May 31, 2018), the court held that "the concrete interest underlying BIPA is the protection and security of biometric data." *Id.* at *5. The *Howe* court held that an employee who "voluntarily submitted to a fingerprint scan" when he was first hired and

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

"then scanned his fingerprint at the beginning and end of each work day" did not suffer any harm to this interest because the employee's "fingerprints were collected in circumstances under which any reasonable person should have known that his biometric data was being collected." *Id.* at *6. The court reasoned that "proper compliance with BIPA's disclosure and written authorization requirements would only have made explicit what should have already been obvious," and any "procedural violations…were not connected to any harm to the security or privacy of the plaintiffs' biometric data." *Id.* at *6.

Additionally, *Aguilar v. Rexnord LLC*, No. 17 CV 9019, 2018 WL 3239715 (N.D. Ill. July 3, 2018), held that the plaintiff had not suffered injury to any privacy right where he "knew his fingerprints were being collected because he scanned them each time he clocked in and out at work, and it was clear that the fingerprints were stored since they were used for authentication purposes." *Id.* at *3. *See also Goings v. UGN, Inc.*, No. 17-CV-9340, 2018 WL 2966970, at *4 (N.D. Ill. June 13, 2018) (dismissing BIPA claim where employee knowingly scanned his handprint each day to clock in and out of work).

These courts' conclusions that a plaintiff cannot bring a BIPA claim based on the knowing and consensual exchange of alleged biometric information comports with BIPA's requirement that only an "aggrieved" person has a right of action. In contrast, the expansive reading of BIPA that Plaintiff advocates could have the effect of imposing massive financial liability on employers—$1,000 to $5,000 per "violation"—for conduct that employees knowingly and voluntarily engage in at least twice each workday to be paid. Plaintiff's proposed reading could make Illinois employers subject to liability merely

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

because notice was provided and consent was obtained either verbally or through employees' conduct, rather than "in writing."

This Court has made clear that "the process of statutory interpretation should not be divorced from a consideration of the 'real-world activity' that the statute is intended to regulate," and an interpretation of a statute that "produces decidedly absurd results" must be rejected. *People v. Hanna*, 207 Ill. 2d 486, 500-03 (2003). Plaintiff's request to interpret BIPA in a way that could saddle employers with potentially devastating financial liability for engaging in conduct *to which employees consented* would be an absurd result and would not advance any statutory or public interest. BIPA should not be read to provide a cause of action for persons who knowingly provide their information, such as foodservice industry employees who use a finger, hand, or facial scan to clock in and out of work or operate a POS system every workday.

II. THERE IS NO INHERENT PRIVACY RIGHT IN FINGERPRINTS, HANDPRINTS, OR FACIAL SCANS.

Plaintiff's brief and the briefs of *amici* the Electronic Privacy Information Center and the American Civil Liberties Union depend on the erroneous premise that "biometric information," such as fingerprints and facial geometry, are particularly sensitive and deserve special privacy protections. The text of BIPA does not support that view. Moreover, Illinois case law has historically rejected the idea that a person can have any reasonable expectation of privacy in his or her fingerprints or facial characteristics. The legislature's choice to limit a cause of action to an "aggrieved" person must be read in the context of the common law's longstanding refusal to recognize any special privacy interest in fingerprints or facial features per se.

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

A. BIPA Does Not Create New Privacy Rights.

Plaintiff and her *amici* summarily claim that BIPA itself creates "privacy rights." However, other than in its title, BIPA does not reference, define, or use the term "privacy." *See generally* 740 ILCS 14/1 *et seq*. Moreover, nowhere in the entire text of BIPA does the legislature state that it intended to create any rights, privacy or otherwise. *See generally id.* "'For a statute to create...private rights, its text must be phrased in terms of the persons benefited.'" *McCready v. White*, 417 F.3d 700, 703 (7th Cir. 2005) (quoting *Gonzaga Univ. v. Doe*, 536 U.S. 273, 284 (2002)). The provisions Plaintiff seeks to enforce are all phrased in terms of obligations placed on "private entit[ies]," not in terms of rights created for individuals. *See* 740 ILCS 14/15. To the contrary, a private right of action under BIPA is limited to a person who is "aggrieved" by a violation, not merely someone who wishes to enforce the terms of the statute. 740 ILCS 14/20. BIPA's "Legislative Findings" section contemplates only one type of injury—"compromise"—meaning identity theft. 740 ILCS 14/5(c).

Because the provisions Plaintiff seeks to enforce are phrased only as obligations on private entities, Plaintiff cannot argue she is "aggrieved" based on purported "privacy rights" that BIPA simply does not create. *See McCready*, 417 F.3d at 703-04 (rejecting plaintiff's attempt to compel disclosure of records under statute regulating conditions under which records must be disclosed, where portion of statute creating private right of action referred only to enforcement by "persons whose information has been disclosed improperly"). For example, this Court has rejected a party's attempt to sue to enforce a statutory licensure scheme where the party was unable to show it was "directly affected" by issuance of a license to a competitor that was allegedly in violation of the statute. *See American Surety Co. v. Jones*, 384 Ill. 222, 229-30 (1943).

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

B. Finger, Hand, and Face Scan Time-Clock and POS Systems Do Not Implicate Any Alleged Privacy Interests Under Illinois Common Law.

Recognizing any new privacy interests in the type of information at issue in the numerous cases pending against employers involving knowing and consensual finger, hand, or facial scans for timekeeping or POS purposes is wholly inconsistent with applicable law. The U.S. Supreme Court has expressly rejected the notion that there is any innate privacy interest in "physical characteristics," such as facial characteristics, that "are constantly exposed to the public." *United States v. Dionisio*, 410 U.S. 1, 14 (1973). In reaching this conclusion, the *Dionisio* court explained that "[n]o person can have a reasonable expectation that … his face will be a mystery to the world." *Dionisio*, 410 U.S. at 14.

This Court has approved of *Dionisio*'s conclusion "that a person has no expectation of privacy in those of his physical characteristics which are commonly exposed to the public." *In re May 1991 Will Cty. Grand Jury*, 152 Ill. 2d 381, 389 (1992). Furthermore, despite holding that "the Illinois Constitution offers greater protection against the invasion of an individual's privacy rights than does the Federal Constitution," this Court has rejected the notion that a grand jury must have probable cause before compelling a witness to produce "physical evidence of a noninvasive nature, such as an in-person appearance in a lineup or fingerprinting." *Id.* at 390-93. Instead, a witness may be compelled to provide fingerprint and handprint evidence upon only "some showing of individualized suspicion as well as relevance." *Id.* at 393. In reaching this conclusion, this Court explained that "[a]n individual has some expectation that members of the public will scrutinize his physical characteristics, noting his bodily structure, his facial features, and the color of his

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

skin," and "fingerprinting, and appearance in lineups leave the individual's body undisturbed." *Id.* at 399.

In the context of privacy torts, Illinois courts have similarly rejected the notion that a person can have a privacy interest in something that is readily available to the public. For example, the court in *Jacobson v. CBS Broad., Inc.*, 2014 IL App (1st) 132480, ¶¶ 45-52, rejected privacy claims where the plaintiff and her children had been videotaped in their bathing suits around a pool in a private backyard. Although "the pool was surrounded by a six foot fence," and the video footage had been shot from inside a neighbor's home rather than from a public area, the court held the plaintiff had no "legitimate expectation of privacy or seclusion," because "the lot lay at the bottom of an incline" and consequently could be seen from "from the public sidewalk or the grassy area behind the…property." *Id.* at ¶¶ 48-49. In other words, the plaintiff lacked any protectable privacy interest because the video footage simply reflected her physical appearance, which was exposed to the public due to the positioning of the property—even though the video footage had not been recorded from a public area. *See also Schiller v. Mitchell*, 357 Ill. App. 3d 435, 441 (2nd Dist. 2005) (24-hour video surveillance of neighbor's home did not support privacy claim where recorded areas could also be seen from public street).

In short, Illinois law does not recognize any privacy interest in physical characteristics such as fingerprints or one's appearance precisely because they are constantly subject to public exposure. A person's face is exposed to the public every time he/she leaves the house, and fingerprints are left on every surface a person touches throughout the day. In fact, fingerprints are so readily available that fingerprint collection kits are sold as children's toys for about $10. *See, e.g.*, https://www.amazon.com/4M-

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

3446-Fingerprint-Kit/dp/B000GKU7BG/ref=sr_1_3?ie=UTF8&qid=1535423526&sr=8-3&keywords=fingerprint+kit (last visited Aug. 27, 2018).

Plaintiffs in these BIPA cases do not allege that they wear a mask and gloves every time they leave their homes to preserve the privacy of their facial features and fingerprints. If the government can compel a person to produce evidence about their fingerprints and physical appearance even absent probable cause, and Illinoisans expose their fingerprints and facial features to the public every day they leave their homes, then certainly there is no injury to any privacy interest when an Illinois employee knowingly and voluntarily provides that same information to his or her employer.

This Court need not decide whether any capture or collection of facial features or fingerprints under any circumstance potentially could implicate a privacy interest under Illinois law. The avalanche of BIPA cases arising from time-clocks and POS systems present a much narrower issue: these employees not only have exposed their visible physical characteristics to public view, but they specifically have permitted them to be scanned by the time-clocks multiple times a day. There is no support under Illinois law for finding an injury to a privacy interest in this context.

Moreover, the scan-based technology used in the employment setting actually affords a significant amount of protection to finger, hand, and facial scan data. Time-clocks and POS systems used in the workplace do not store fingerprints, handprints, or facial images, but rather scan the employee's fingertip, hand, or face and create an encrypted algorithm (called a template) that the scanning system then uniquely associates with that employee. To *amici*'s knowledge, there is not a single BIPA case alleging that any employer's database has been breached—much less that any employee has experienced

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

identity theft as a result of using scan-based technology in the workplace. Nor is there a single BIPA case alleging that finger, hand, or face scan data has been used or disclosed for any purpose other than timekeeping or POS purposes. There similarly is not a single BIPA case where an employee alleges he or she objected to providing finger, hand, or face scans when the employer initially requested them—and many cases involve employees who have been knowingly and voluntarily scanning their fingers, hands, or faces for many years for timekeeping and pay purposes. Employers use care in collecting, storing, and using scan-based data, affording this information much greater protection than the Illinois courts have historically provided. Employers who have taken such great care to protect information that Illinois law has never even recognized as private should not be punished with massive statutory penalties in the absence of any alleged harm to employees.

C. Plaintiff's Allegations Do Not Implicate Any Other Privacy Interest Recognized By Illinois Law.

Not only has this Court expressly rejected the notion that physical features deserve heightened privacy protections, this Court also has made clear that a plaintiff cannot pursue a privacy-related cause of action unless that plaintiff satisfies the elements of a recognized privacy tort. *See Lovgren v. Citizens First Nat'l Bank*, 126 Ill.2d 411, 416-19 (1989) (engaging in extensive analysis of whether plaintiff's allegations could satisfy elements of any recognized privacy tort). *See also, e.g.*, *Maglio v. Advocate Health & Hosps. Corp.*, 2015 IL App (2d) 140782, ¶ 31, *appeal denied*, 396 Ill. Dec. 177 (Ill. 2015) (refusing to recognize invasion of privacy claim based on theft of medical information "because case law requires actual disclosure to a third party and plaintiffs have made no such allegations"); *Cooney v. Chicago Public Schools*, 407 Ill. App. 3d 358, 366-67 (1st Dist. 2010) (explaining that Illinois law recognizes only four privacy torts and dismissing

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

privacy claims where plaintiff failed to allege all elements of one of those torts); *Busse v. Motorola, Inc.*, 351 Ill. App. 3d 67, 71-72 (1st Dist. 2004) (same).

Under Illinois law, a defendant cannot intrude on a plaintiff's privacy rights where the plaintiff has voluntarily given the information at issue to the defendant. *See Dwyer v. Am. Express Co.*, 273 Ill. App. 3d 742, 746 (1st Dist. 1995) (affirming dismissal of claims because "a cardholder is voluntarily, and necessarily, giving information to defendants that, if analyzed, will reveal a cardholder's spending habits and shopping preferences"). The same is true in employment—there is no privacy interest in information knowingly and voluntarily provided to an employer, no matter how sensitive the information. *Miller v. Motorola, Inc.*, 202 Ill. App. 3d 976, 981 (1st Dist. 1990). For example, the plaintiff in *Miller* told her employer that she was having a mastectomy and reconstructive surgery, and the employer later told the plaintiff's coworkers about the surgeries, despite having promised the plaintiff that it would keep her medical information confidential. *Id.* at 978-79. The court held the plaintiff could not state a claim for intrusion on seclusion because "[t]he alleged wrongful actions involve dissemination or publication of information voluntarily provided to defendant by plaintiff, not defendant's unauthorized intrusion." *Id.* at 981. The plaintiff consequently was limited to attempting to pursue a claim for public disclosure of private facts based on the employer's alleged dissemination of the information. *Id.* In other words, the plaintiff's voluntary provision of allegedly sensitive information to her employer precluded any privacy claim unless the plaintiff could also show the employer publicly disclosed the information. Because voluntarily providing information to one's employer eviscerates any claimed privacy right in the information, a

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

plaintiff who chooses to provide purported biometric information to an employer for timekeeping and POS purposes cannot sustain a privacy claim.

Furthermore, Illinois common law has never recognized an innate privacy right in personal information, even when such information is disclosed, absent an allegation of identity theft.[2] For example, the First District in *Cooney* addressed a situation in which the defendant accidentally disclosed names, addresses, Social Security numbers, marital status, and health-related information for more than 1,700 former employees. *Cooney*, 407 Ill. App. 3d at 360. *Cooney* explained that Illinois does not recognize any common law "duty to protect plaintiffs' information from disclosure." *Id.* at 363. The *Cooney* court dismissed claims alleging an "increased risk of future identity theft" and "costs of credit monitoring services" because "[w]ithout more ... the plaintiffs have not suffered a harm that the law is prepared to remedy." *Id.* at 365-66 (quoting *Pisciotta v. Old National Bancorp.*, 499 F.3d 629, 639 (7th Cir. 2007)). *See also Busse*, 351 Ill. App. 3d at 71–73 (holding that disclosure of names, phone numbers, addresses, social security numbers, and cell phone usage information did not support privacy claim).

Similarly, *Maglio* involved a situation where computers containing the "names, addresses, dates of birth, social security numbers, health insurance data, Medicare and Medicaid data, medical diagnoses, diagnosis codes, and medical record numbers" of 4 million patients were stolen from the defendant's office. *Maglio*, 2015 IL App (2d) 140782, ¶¶ 3-5. The plaintiffs claimed that because medical information was "inherently

[2] At least one court has expressed skepticism that biometric information could be used to perpetrate identify theft. *See Doporcyk v. Roundy's Supermarkets, Inc.*, No. 17 C 5250, Dkt. #80 (July 16, 2018) (attached as Exhibit 1) ("[T]he court is skeptical of any analogy between a finger print and the personal information at issue in *Gubala* that could be used to steal a person's identity (i.e., social security number, credit card information).").

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

personal and particularized to the individual," they had some type of implicit privacy interest when the information was stolen. *Id.* at ¶ 27. *Maglio* rejected this argument, reasoning "there has been no known public disclosure or identity theft or fraud with respect to plaintiffs' data"—rendering the information's private nature irrelevant to the underlying legal claims. *Id*. at ¶¶ 27-28, 31. Because Illinois does not recognize a privacy right in factual information used to identify a person, an employee cannot claim any privacy interest in the factual information—physical characteristics such as fingerprints, handprints, or facial features—used to identify them for timekeeping and POS purposes.

III. IMPOSING LIABILITY ON EMPLOYERS ABSENT ANY HARM TO EMPLOYEES WOULD CREATE A DUE PROCESS PROBLEM AND DOES NOT ADVANCE BIPA'S GOALS.

If BIPA is applied as proposed by Plaintiff and her *amici*, it would deprive Illinois employers of due process rights by allowing plaintiffs who consented to collection of their biometric information and suffered no injury to impose extraordinary monetary liability on their employers. This Court has explained that a statute violates a defendant's due process rights under the Illinois Constitution when the statute is not "reasonably designed to remedy the evils which the legislature has determined to be a threat to the public health, safety and general welfare." *People v. Bradley*, 79 Ill.2d 410, 417 (1980) (internal quotation marks omitted). Here, BIPA's preamble indicates that the purpose of the statute is to encourage the growth and use of biometric technology by addressing consumers' hesitancies about such technology. In particular, the legislature found that the use of biometric technology "appears to promise streamlined financial transactions and security screenings," but that "members of the public are weary of the use of biometrics when such information is tied to finances or other personal information" and "many members of the public are deterred from partaking in biometric identifier-facilitated transactions" due to

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

concerns about the data being "compromised." 740 ILCS 14/5(a), (c), (d), (e). In other words, the legislature's explicit intent is to reduce consumers' wariness about this "promis[ing]" technology.

Use of finger, hand, or facial scans in the employment setting does indeed provide many benefits to both employers and employees. For example, scan-based timekeeping and POS technology in the workplace allow for faster and more accurate authentication than traditional methods such as requiring employees to supply usernames and passwords. It eliminates the delay, inconvenience, and security risks caused if an employee loses an ID card used for authentication purposes. It also cuts down on timekeeping mistakes and fraud by ensuring that the employees using the scan-based system truly are who they say they are, and not using other employees' ID cards or passwords. This, in turn, ensures that employees are fully and accurately paid for all time worked.

Plaintiff and her *amici* argue that BIPA's purpose is to protect consumers and employees. They do not and cannot argue, however, that BIPA is meant to bankrupt Illinois employers who implemented finger, hand, or facial scan timekeeping to *protect employees* by ensuring that such employees accurately record and are paid for time worked. In implementing such systems, employers are complying with state and federal wage and hour laws, activities that should be encouraged, not punished by BIPA. *See Brazinski v. Transp. Serv. Co.*, 159 Ill. App. 3d 1061, 1067 (1st Dist. 1987) ("[I]t is the public policy of the State to ensure the proper payment of wages to employees by employers."); *People ex rel. Dep't of Labor v. K. Reinke, Jr. & Co./Reinke Insulation*, 319 Ill. App. 3d 721, 727 (1st Dist. 2001) (explaining that Illinois wage and hour laws "inure[] to the benefit of Illinois workers and taxpayers").

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

Allowing purely statutory violations of BIPA to create liability for employers would subject employers to liquidated damages of $1,000 or $5,000 per BIPA "violation"—a term that is not defined in BIPA and which many BIPA plaintiffs are contending is payable for each separate time an employee clocks in or out of work or operates a POS system. This would create massive liability exposure for Illinois employers even though no harm is alleged and the benefits received by employees are substantial. Such a result would not reasonably advance BIPA's goals of encouraging the use of biometric technology. Nor would it serve to reduce the risk of any "compromise" of biometric data, as employees in the time-clock cases all allege they already knew they were providing their finger, hand, or facial scans to their employer for the purpose of tracking their work time. Because Plaintiff's proposed interpretation would impose potentially devastating liability on employers without any countervailing benefit to employees—who already knowingly consent to providing their finger, hand, or facial scans—Plaintiff's proposed interpretation would violate employers' due process rights. *See Bradley*, 79 Ill. 2d at 417–18 (holding statute violated due process where penalty was "not reasonably designed to remedy the evil" the legislature identified); *People v. Morris*, 136 Ill. 2d 157, 161–62 (1990) (holding statutory penalty unconstitutional where it did not advance legislature's stated purpose in enacting statute).

CONCLUSION

The expansive interpretation of BIPA that Plaintiff proposes must be rejected. Employees who knowingly and willingly scan their finger, hand, or face to clock in and out of work or to operate a POS system every workday simply are not "aggrieved." Neither the text of BIPA nor Illinois case law support treating fingerprints, handprints, or facial scans as deserving of special privacy protections because Illinoisans constantly expose

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

these purported "biometric identifiers" to the public every day. Moreover, reading BIPA to impose massive monetary penalties on employers despite employees' consent and the absence of any injury would violate employers' due process rights.

Dated: September 11, 2018

Respectfully submitted,

/s/ *Melissa A. Siebert*

Melissa A. Siebert
ARDC #6210154
Bonnie Keane DelGobbo
ARDC #6309394
BAKER HOSTETLER LLP
191 North Wacker Drive, Suite 3100
Chicago, IL 60606
(312) 416-6200
msiebert@bakerlaw.com
bdelgobbo@bakerlaw.com

Attorneys for Amici Curiae Restaurant Law Center and Illinois Restaurant Association

Angelo I. Amador
Restaurant Law Center
2055 L Street, NW
Suite 700
Washington, DC 20036
(202) 492-5037
aamador@restaurant.org

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

CERTIFICATE OF COMPLIANCE

I certify that this brief conforms to the requirements of Rules 341(a) and (b). The length of this brief, excluding the pages or words contained in the Rule 341(d) cover, the Rule 341(h)(1) statement of points and authorities, the Rule 341(c) certificate of compliance, the certificate of service, and those matters to be appended to the brief under Rule 342(a), is 4,992 words.

/s/ *Melissa A. Siebert*
Melissa A. Siebert

Attorney for Amici Curiae Restaurant Law Center, Illinois Restaurant Association, and National Retail Federation

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

EXHIBIT 1

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

THOMAS DOPORCYK, on behalf of himself and others similarly situated, Plaintiff, v. ROUNDY'S SUPERMARKETS, INC.; ROUNDY'S ILLINOIS, LLC, dba MARIANO'S; and THE KROGER COMPANY, Defendants.	No. 17 C 5250 Judge Thomas M. Durkin

ORDER

The Court is concerned that Plaintiff has failed to allege an injury in fact sufficient to support the Court's constitutional jurisdiction. *See Spokeo, Inc. v. Robins*, 136 S. Ct. 1540 (2016). A court in this district recently remanded claims for violation of the Illinois Biometric Information Privacy Act for failure to allege constitutional standing. *See Howe v. Speedway LLC*, 2018 WL 2445541 (N.D. Ill. May 31, 2018). Each party should file a brief of no more than 10 pages addressing this issue by August 17, 2018. The parties should exchange draft briefs on August 10, 2018 so that the final briefs they file with the Court address each others' arguments. No responses will be permitted.

The Court is cognizant that this issue puts the parties in somewhat of a procedural bind. *See Barnes v. ARYZTA, LLC*, 288 F. Supp. 3d 834 (N.D. Ill. 2017). Generally, plaintiffs want to demonstrate that they have suffered an injury in fact,

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM

but here lack of an injury in fact under the federal Constitution would result in remand, which is the forum Plaintiff prefers. Similarly, although defendants in federal court are generally happy to take the dismissal order that comes with a finding that the plaintiff has failed to allege an injury in fact, Defendants here (presumably) oppose remand and represented in their notice of removal that the Court has subject matter jurisdiction.

One additional point: To the extent Plaintiff hopes to argue that he has been injured by the "release" or "dissemination" of his "personal information," *see Gubala v. Time Warner Cable, Inc.*, 846 F.3d 909, 912 (7th Cir. 2017), Plaintiff should know that the Court is skeptical of any analogy between a finger print and the personal information at issue in *Gubala* that could be used to steal a person's identity (i.e., social security number, credit card information). This is not intended to prohibit Plaintiff from arguing that such an analogy is reasonable, but just to provide notice that such an argument will be difficult.

ENTERED:

Honorable Thomas M. Durkin
United States District Judge

Dated: July 16, 2018

SUBMITTED - 2151281 - Melissa Siebert - 9/18/2018 10:28 AM