BIOMETRICS AND BEYOND

THE EVOLUTION OF WORKPLACE PRIVACY ISSUES

◆◆◆◆◆◆

Wade M. Fricke (Moderator) – Ogletree Deakins (Cleveland)

Wes Carlisle – Dhanani Group

Keith E. Kopplin – Ogletree Deakins (Milwaukee)

Anne E. Larson – Ogletree Deakins (Chicago)
Overview

Since the advent of motion pictures, filmmakers and moviegoers have been fascinated by projections of the future. In 1987, for example, the movie *RoboCop* depicted a police officer who had been killed in the line of duty revived as a cyborg law enforcement officer retrofitted with an exoskeleton providing super-human strength, onboard computers, and vision enhancements with the aim of cleaning up the streets of crime-ridden Detroit, Michigan.

A few years later, in 1990, *Total Recall* offered a glimpse into life on Mars, as Arnold Schwarzenegger’s character, embroiled in espionage, found himself unable to determine if his experiences were real or the result of memory implants. In one memorable scene, Schwarzenegger’s character removes a walnut-sized tracking implant that had been embedded in his skull.

*Minority Report*, a 2002 Steven Spielberg film, stars Tom Cruise as a police officer on the run in the year 2054. The movie depicts a futuristic society where biometric scanners are everywhere. Surveillance isn’t just by the government but also by businesses. Cruise walks through a mall where iris scanners bombard him with targeted ads: “John Anderson, you look like you could use a Guinness right about now.” When he walks into the GAP, he hears: “Welcome back to the GAP. How did those tank tops work out for you?” The film is filled with flashing ads and an endless barrage of stimulation prompted by Cruise’s biometric data. Cruise ultimately resorts to an eye transplant to conceal his identity while seeking to exonerate himself. The film ultimately depicts the dangers of biometric identification and asks what harm may befall us if our biometric data falls into the wrong hands.

In 2019, biometric identifiers and equipment, microchipping, and wearable data collection and tracking technology are no longer the stuff of science fiction or the tools of Bond villains set in the year 2054. For example, many of us routinely use biometric finger scans to log into our smart phones, to access our online checking accounts, or to buy coffee at Starbucks. In response to lingering privacy and security concerns, however, some states have enacted legislation that regulates the use and destruction of such biometric data.

In 2008, Illinois became the first state to enact legislation regulating a private entity’s collection, use, storage, and destruction of biometric data with the Illinois Biometric Information Privacy Act (BIPA). BIPA gives individuals a private right of action and statutory damages of $1,000 per negligent violation, $5,000 per intentional violation, actual damages (if greater than the statutory damages), injunctive relief, and attorneys’ fees. The private right of action, statutory damages and attorneys’ fees give BIPA class action potential. The consumer class actions began in 2015 with over 30 to date. The employer class actions followed two years later in 2017, with over 220 filings to date. As of March 31, 2019, more than 250 BIPA class actions have been filed.

BIPA lacks clarity in numerous respects. It has no statute of limitations and no court has yet ruled on this issue. BIPA fails to define “aggrieved,” which led to years of litigation over what the legislature meant by a “person aggrieved by a violation of this Act,” until the recent Illinois

---

1 740 ILCS 14, et seq.
2 Id.
Supreme Court decision in *Rosenbach*. BIPA also fails to define “violation” which renders it subject to different interpretations such as whether a violation could be (1) per company, (2) per facility, (3) per employee, (4) per employee multiplied by each statutory subsection purportedly violated, or (4) per employee multiplied by each use of the biometric scanner (i.e., each clock-in and clock-out).

In 2009, Texas enacted the Texas Capture or Use of Biometric Identifier Act (“Texas Act”), which is modeled in large part after BIPA. Unlike BIPA, the Texas Act does not give individuals a private right of action, statutory damages or attorney’s fees but instead empowers the attorney general to bring an action to recover a “civil penalty of not more than $25,000 for each violation.” Like BIPA, the Texas Act does not define “each violation” so it is unclear how large a civil penalty the attorney general may impose.

In 2017, Washington followed Illinois and Texas and enacted a statute regulating the collection and use of biometric information. The Washington statute follows the Texas Act by not giving individuals a private right of action and instead providing for enforcement by the attorney general. A number of other states have proposed or considered such biometric legislation. Still other states regulate the unauthorized disclosure or hacking of biometric data as part of existing data privacy laws, as discussed more thoroughly herein.

Microchipping and wearable technology have also risen to the forefront of state legislatures’ attention and the national news. Currently, California, Missouri, North Dakota, Oklahoma, and Wisconsin prohibit tagging individuals without their consent. Other states have considered similar legislation and some, like Wisconsin, have proposed legislation specifically targeted at employers, and require written employee consent and the employer to cover costs of implantation and removal. Similarly, wearable technology presents issues related to privacy and voluntariness, with state and federal laws focusing on GPS tracking and involuntary participation in wellness programs.

**Microchipping**

1. **Applications and Uses**

Perhaps the primary appeal of microchipping is its ability to provide individuals with instant access to facilities, equipment, and accounts. By embedding a microchip containing data such as an individual’s securing clearance or commissary account number, companies can ensure instant access while minimizing security breaches caused by lost or stolen key fobs, ID badges, and other external access credentials. While microchipping is in its infancy, experts predict that in the coming years large technology companies will begin implementing the

---

4 TEX. BUS. & COM. CODE §§503.001, *et seq.*
5 TEX. BUS. & COM. CODE §503.001(d).
6 WASH. REV. CODE §§19.01, *et seq.*
7 CAL. CIVIL CODE §52.7(A).
8 MO. REV. STAT. §285.035.
9 N.D. CENT. CODE §12.1-15-06.
10 OKLA. STAT. TIT. 63 §1-1430
11 WIS. STAT. §146.25.
convenient devices and in so doing normalize what are now relatively few and even stigmatized devices.\textsuperscript{12}

\section{Media Attention}

However, the tug of war between microchipping’s apparent ease of access and the drawbacks related to privacy and consent have raised the hackles of many lawmakers and commentators. For example, Three Square Market, a Wisconsin vending machine technology company, microchipped 95 percent of its workforce—to critical media fanfare—and claimed that microchip implantation was an innovative portion of its business model making employees’ and potentially customers’ lives easier.\textsuperscript{13} The rice-sized microchips acted as the conductor in a multistage feedback network allowing employees to login to their computers, but only if they used the chip to scan into the company’s office building. Three Square Market’s President and CEO touted the technology as a significant advance for security and efficiency, while critics viewed its potential for privacy infringement as its main drawback.\textsuperscript{14}

\section{Legal Issues}

As made obvious by the heated national attention paid to Three Square Market’s implantation of microchips in most of its employees’ hands, implanting employees with a microchip or similar technology presents complex ethical, privacy, and business-need questions debate around the subject will continue.

At the top of the heap of these issues are questions regarding consent. Those states that expressly prohibit the involuntary implantation of a microchip device—California,\textsuperscript{15} Missouri,\textsuperscript{16} North Dakota,\textsuperscript{17} Oklahoma,\textsuperscript{18} and Wisconsin\textsuperscript{19}—also impose steep fines on those that violate the statute. For example, in Oklahoma and Wisconsin violators face fines of $10,000 for each violation and each day of continued violation constitutes a separate offense. California is a bit more lenient, imposing fines of up to $1,000 for each day of continued violation and capping fines for each offense at $10,000. Important to note is all those states banning microchipping only prohibit the \textit{involuntary} implantation of a microchip device, leaving employers and employees free to implant microchips with employee consent. What “consent” means and acceptable kinds of information that is collected, stored and used will continue to develop as the ubiquity of microchipping increases.

\begin{thebibliography}{1}

\bibitem{12} See you will get chipped—eventually. \textsc{USA Today}, https://www.usatoday.com/story/tech/2017/08/09/you-get-chipped-eventually/547736001/ (last visited March 19, 2019).


\bibitem{15} \textsc{Cal. Civil Code} §52.7(A).

\bibitem{16} \textsc{Mo. Rev. Stat.} §285.035.

\bibitem{17} \textsc{N.D. Cent. Code} §12.1-15-06.

\bibitem{18} \textsc{Okla. Stat. Tit.} 63 §1-1430

\bibitem{19} \textsc{Wis. Stat.} §146.25.
\end{thebibliography}
Additional legal concerns include religious discrimination regarding individuals who may have sincerely held religious beliefs opposing piercings or immunizations and workers’ compensation.

Wearables in the Workplace

1. Applications and Uses

Wearable monitoring technology can be as common place as a fitness tracker that monitors physical activities, to the more specialized, like smart hats, that monitor the fatigue levels of workers. In general wearable technology can provide useful information to employers aimed at minimizing health and safety risks to employees, enhancing employee wellness, increasing productivity, managing workflow and increasing efficiency, minimizing, leave abuse, controlling access to facilities and equipment and fulfilling timekeeping obligations. Inevitably these devices collect or use personal data from employees, which could trigger similar concerns as discussed above regarding microchipping—consent, privacy, and unwanted knowledge about employee activities.

2. Media Attention

In early 2018, Amazon was awarded two patents for a wristband that can pinpoint the location of warehouse employees and track their hand movements in real time. The patents describe an inventory management system comprised of trackers and receivers used to monitor workers’ performance. The system includes ultrasonic devices placed around the warehouse, the wristbands themselves, and a management module that oversees everything. The wristbands also feature an ultrasonic unit that’s used to track where the worker is in relation to any particular inventory bin. If their hands are moving to the wrong item, the bracelet will buzz. Although the patent descriptions characterize the wristbands as a means to collect data about inventory, critics took aim at the inevitability of collecting employee personal data.20

Boeing, in an effort to maximize employee efficiency and reduce errors in its wiring systems, implemented a pilot program in 2016 utilizing Google Glass, Google’s brand of smart glasses that project a display on a wearer’s glasses lens. Aircraft wiring system technicians at Boeing had used PDF “maps” to navigate a complex wiring system and wasted time searching the map on their computer screen and then turning back and applying that information back onto the physical wiring system on which they worked. By implementing Glass, Boeing aimed to save time by projecting images of the wiring system directly onto a technician’s glasses and implementing supporting applications to allow the wearer to use touch gestures and voice commands to navigate the wiring maps hands free.21

3. Legal Issues

A wearable’s GPS tracking capabilities could trigger improper surveillance and invasion of privacy concerns. While surveillance of employees in observable places like public streets or an employee’s yard is still generally lawful, surveillance into the windows of an employee’s


home is illegal. Moreover, in some states if the wearable tracks GPS data, the employer must disclose this information. For example, in Wisconsin it is illegal for a private individual to obtain information about another person’s movement or location through a GPS device without the other person’s consent.

Collection of wellness information through wearables is permitted by the Americans with Disabilities Act (ADA) and Title II of the Genetic Information Nondiscrimination Act of 2008 (GINA), provided that any information is collected with employee consent. It is unclear the extent to which monetized incentive programs will be permitted, however, as the U.S. District Court for the District of Columbia ordered the U.S. Equal Employment Opportunity Commission (EEOC) to vacate its 2016 rules permitting that an incentive limit of 30 percent of the cost of coverage rendered an employee health program voluntary rather than involuntary.

Biometric Data Collection and Use

1. Applications and Uses

By one definition, “biometrics” is “the measurement and analysis of unique physical and behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity.” Therein lies the appeal associated with biometric information. Unlike usernames and passwords, biometric information is unique to an individual and not subject to change. For that reason, biometric information is often viewed as an infallible way to verify personal identity and authenticate transactions.

According to Spiceworks, a professional network for the information technology industry, 62% of businesses currently use some form of biometric authentication. By the year 2020, that number is projected to increase to 90%. While fingerprint-scanning technology still accounts for the majority of corporate biometric authentication (57%), businesses are also using facial recognition (14%), hand geometry recognition (5%), and voice recognition (2%).

In the workplace, biometrics can be used to access buildings, log onto computers, or operate pieces of equipment. It can also be used to record hours of work for payroll purposes. These are typical areas in which employers have a vested interest in confirming that the transaction actually relates to the individual associated with the record. Whereas a security access badge, pin number, or key fob can be lost or stolen, fingerprints and retinal scans cannot be “misplaced” by the employee, providing the employer with confidence that the records created by biometric authentication truly belong to the individual associated with the record.

---

22 Vail v. Raybestos Products Co., 533 F.3d 904 (7th Cir. 2008) (holding that employer entitled to terminate because it investigated and confirmed an “honest suspicion” that employee was abusing leave by hiring off-duty cop to observe plaintiff doing yard work when she had called in that day with a migraine); Munson v. Milwaukee Bd. of School Directors, 969 F.2d 266 (7th Cir. 1992) (no invasion of privacy when employer photographs or films an employee in a public place open to the public where employee was observed from public streets to ascertain his residence).

23 Wis. Stat. §940.315(1)(a). Note, however, that an employer can place a GPS on a company owned or leased vehicle and track GPS movement of that vehicle used by company employees. See also Wis. Stat. §955.50.


A security firm called BioCatch has even introduced a method of detecting computer fraud by first creating a biometric profile of computer users based on things like how they hold a telephone, whether they type with one or two hands, and how they scroll or toggle between screens.\textsuperscript{27} The profile reflected by the behavioral biometrics is then compared to subsequent computer use activity in order to identify when a different individual is using the computer. While this could simply be a different authorized user, it could also be an indication that the system has been compromised.

2. **Media Attention**

While the immutable nature of biometric information makes it appealing for a business looking for certainty regarding the authenticity of key transactions, it also makes it ripe for hackers and identity thieves. Again, user names and passwords can be changed, security badges and key fobs replaced, but biometric information is permanent. As such, hackers and thieves can acquire the information at their convenience but wait to utilize it until a more opportune time, once the victims of the breach have been lulled into believing that their information – indeed their identity – is secure. Recent media attention highlights this concern.

- In September 2013, Apple launched the new iPhone 5s, with TouchID, a fingerprint sensor described as “an innovative way to simply and securely unlock your phone with just the touch of a finger.”\textsuperscript{28} Within weeks, however, a group from Germany called the Chaos Computer Club claimed they had successfully bypassed the TouchID feature on an iPhone 5s by taking a photograph of a latent fingerprint of the user, and recreating a “fake fingerprint” that could be put onto a film and used to unlock the device.\textsuperscript{29}

- As a matter of national security, many employees of the federal government are subjected to extensive background screens for which their fingerprints are collected. In September 2015, the United States Office of Personnel Management (OPM) reported that 5.6 million fingerprints of government employees had been hacked, along with 21.5 million Social Security numbers.\textsuperscript{30} According to a press release issued by OPM at the time, “Federal experts believe that, as of now, the ability to misuse fingerprint data is limited. However, this probability could change over time as technology evolves.”


In March 2018, a number of airlines, including British Airways and Lufthansa, announced that they would begin testing the use of biometric information, including fingerprints and facial recognition, to facilitate the boarding process.

3. Legal Issues

a. Illinois Biometric Information Privacy Act (BIPA)

The State of Illinois enacted BIPA in 2008 to regulate a private entity's collection, use, storage, transmission and destruction of “biometric identifiers”\(^{31}\) (retina or iris scans, fingerprints, voiceprints, or hand or facial geometry scans) and “biometric information.”\(^{32}\) “Biometric information” is defined broadly to include “any information ... based on an individual’s biometric identifier used to identify an individual.”\(^{33}\)

Section 15 of BIPA prohibits a private entity from collecting a person’s or customer’s “biometric identifier” or “biometric information” unless it first informs them of the “specific purpose and length of term for which [it] is being collected, stored and used” and obtains their executed release or consent.\(^{34}\) Section 15 also requires private entities to develop a written policy that establishes a retention schedule and guidelines for the timely destruction of biometric identifiers or biometric information in compliance with BIPA.\(^{35}\)

Section 15 precludes private entities from selling, leasing, trading, or otherwise profiting from an individual’s biometric identifier or biometric information.\(^{17}\) It also prohibits private entities from making any “unauthorized disclosures” of biometric identifiers or biometric information.\(^{36}\)

As discussed above, Section 20 of BIPA gives a “person aggrieved by a violation of this Act” a private “right of action” to sue for statutory damages of $1,000 per negligent violation, $5,000 per intentional violation, actual damages (if greater than the statutory damages), injunctive relief, attorneys’ fees, and costs.\(^{37}\)

i. Class Actions and Rosenbach

Rosenbach v. Six Flags Entertainment Corp. appears to be the seventh BIPA consumer class action and was filed on January 7, 2016. Stacy Rosenbach, as mother and next friend of Alexander Rosenbach, filed suit against Six Flags after her son visited the amusement park on a school field trip. Ms. Rosenbach learned that Six Flags scanned her son’s thumbprint to allow him access to the amusement park on a season pass. The lawsuit did not allege any actual harm to her son. It alleged that Six Flags failed to inform Alexander or his mother of the specific purpose and length of term for which his fingerprint had been collected, and failed to obtain his written consent or hers prior to collecting it.

\(^{31}\) 740 ILCS 14/10

\(^{32}\) 740 ILCS 14/15.

\(^{33}\) Id.

\(^{34}\) 740 ILCS 14/15(b).

\(^{35}\) Id.

\(^{36}\) Id.

\(^{37}\) 740 ILCS 14/15(d)(1)-(4).
When Six Flags’ initial motion to dismiss was denied, the amusement park sought interlocutory review of the denial. On appeal, the appellate court sided with Six Flags and held that plaintiff must allege some actual harm—not just a violation of the Act—to be a “person aggrieved by a violation of this Act.” If every technical violation of BIPA was actionable, it would render “superfluous” the requirement that a person be “aggrieved by a violation of this Act.”

The Illinois Supreme Court rejected the appellate court’s ruling that actual injury is a prerequisite to the recovery of statutory damages under BIPA. It held this precondition was “antithetical to the Act’s preventative and deterrent purposes” and that a violation of BIPA’s notice and consent provisions was a “real and significant” injury:

> When a private entity fails to adhere to the statutory procedures, as defendants are alleged to have done here, “the right of the individual to maintain [his or] her biometric privacy vanishes into thin air. The precise harm the Illinois legislature sought to prevent is then realized.” This is no mere “technicality.” The injury is real and significant.

*Rosenbach* will continue to propel the flood of BIPA class actions and could transfer millions of dollars from companies that do business in Illinois into the pockets of the plaintiffs’ class action bar. While no one can dispute BIPA’s good intentions, biometric technology appears to have evolved beyond the technology that existed in 2008. The biometric equipment in use today generally uses an algorithm to transform the biometric identifier into a mathematical representation that renders it unreadable and unidentifiable, such as 72E7FAD4CAAB532B4DA6A33B6B3FA. These safeguards prevent much of the harms contemplated by the statute. Thus, laws like BIPA, with its statutory damages and fee-shifting provisions, do not necessarily keep pace with technological advances and may be too blunt an instrument for regulating these issues. What Illinois needs is an amended statute that is not punitive but fairly addresses the statute’s prevention and enforcement concerns— not a law that has the capacity to wreak havoc on the economy and companies that do business in Illinois with multi-million dollar judgments over technical violations.

### b. Other State Statutes Regulating Biometric Data

#### i. New York

New York Labor Law prohibits private employers from *requiring* employees to be fingerprinted as a condition of employment or continued employment, unless otherwise required by law. Section 201-a of the New York Labor Law states:

> Except as otherwise provided by law, no person, as a condition of securing employment or of continuing employment, shall be required to be fingerprinted. This provision shall not apply to employees of the state or any municipal subdivisions or departments thereof, or to the employees of legally incorporated hospitals, supported in whole or in part by public funds or private endowment, or to the employees of medical colleges affiliated with such hospitals or to employees of private proprietary hospitals.


40 *Id.* at ¶34 (citation omitted).
Thus, with limited exceptions, Section 201-a prohibits private employers from requiring employees to be fingerprinted as a condition of securing or continuing employment. Enacted in 1937, the purpose behind the legislation “clearly was to prevent private employers from using fingerprinting as a means for blacklisting union leaders and members.”\(^{41}\)

Although enacted for the reason suggested above, several companies have sought opinions from the New York State Department of Labor (NYSDOL) as to whether the use of a biometric device in a time clock violates Section 201-a. As it turns out, the NYSDOL interprets Section 201-a as prohibiting employers from requiring employees be fingerprinted for timekeeping purposes, and it does not matter that the time clock does not actually store the employees’ fingerprints. According to the NYSDOL, simply interpreting the fingerprint was enough to violate the Labor Law’s protections. Under the NYSDOL’s guidance, requiring the use of a finger-scanning biometric time clock or similar device would violate Section 201-a. But, there are limited exceptions: (i) employees required by law to be fingerprinted (e.g., teachers) may be required to use a biometric time clock for timekeeping purposes, regardless of whether the device interprets the employee’s fingerprints; (ii) time clocks that “measure the geometry of the hand” are permissible so long as they do not scan the surface details of the hand and fingers in a manner similar or comparable to the scanning of a fingerprint; and (iii) voluntary use of a finger-scanning biometric device is permissible. (Note: employers may not take any adverse employment action against employees who forego fingerprinting, or otherwise coerce employees to use the biometric device.)\(^{42}\)

While the NYSDOL’s opinion on this issue is clear, no New York court has weighed in on the use of finger-scanning devices as a timekeeping method. The weight of New York case law, however, favors deference to the NYSDOL and its opinions. Thus, while the courts have not weighed in on the use of biometric devices and Section 201-a, the NYSDOL’s position on this is clear—the use of biometric finger scanning that uses anything other than a scan of finger geometry is prohibited, and it is probable that courts will defer to the NYSDOL’s interpretive guidance.

In addition to its law addressing the use of fingerprints, New York also prohibits an employer from publicly posting an employee’s “personal identifying information,” which includes Social Security Number, home address or telephone number, email address, Internet identification name or password, parent’s surname, and driver’s license number. Although the definition of “personal identifying information” does not yet include personal identifiers such as biometric data, safeguarding such data is a good business practice.

ii. Texas

Under Texas law, a person may not capture biometric information for commercial purposes unless it informs the individual beforehand and obtains the individual’s consent.\(^{43}\) A person who possesses biometric identifiers that are captured for commercial purposes may not sell, lease, or disclose biometric information unless: the individual consents to disclosure for purposes of identification in the event of his or her disappearance or death; the disclosure completes a financial transaction the individual requested or authorized; the disclosure is


\(^{42}\) See NYSDOL Opinion Letters RO-10-0024 (April 22, 2010), RO-08-0029 (August 14, 2008) and RO-08-0091 (August 26, 2008).

required or permitted under federal or state law, or the disclosure is made to law enforcement in response to a warrant.\[^{44}\] In addition, the person who possesses a biometric identifier must store the information using reasonable care in a manner that is the same or more protective than how it stores other confidential information, and it must destroy the information no later than the first anniversary of the date the purpose for collecting the information expires. A business must implement and maintain reasonable procedures, including taking any appropriate corrective action, to protect from unlawful use or disclosure any sensitive personal information collected or maintained by the business in the regular course of business. Personal information includes unique biometric data and Social Security Numbers.

Texas does not provide for a private cause of action under the statute but instead charges its attorney general with responsibility for enforcement.\[^{45}\]

iii. Washington

This year, the State of Washington became the third state to enact a law specifically addressing the use of biometric information. In the new law, the state provides that it “intends to require a business that collects and can attribute biometric data to a specific uniquely identified individual to disclose how it uses that biometric data, and provide notice to and obtain consent from an individual before enrolling or changing the use of that individual’s biometric identifiers in a database.”

The law provides that “a person may not enroll a biometric identifier in a database for a commercial purpose, without first providing notice, obtaining consent, or providing a mechanism to prevent the subsequent use of a biometric identifier for a commercial purpose.”\[^{46}\] The law requires that a “person who knowingly possesses a biometric identifier of an individual that has been enrolled for a commercial purpose” must take “reasonable care” to guard against unauthorized access and may retain the information no longer than is reasonably necessary.\[^{47}\]

Washington does not provide for a private cause of action under the statute but instead charges its attorney general with responsibility for enforcement.\[^{48}\]

iv. California

The California Consumer Privacy Act (CCPA) was enacted on June 28, 2018, and will become effective on January 1, 2020. The CCPA was enacted to protect California residents’ rights to know what personal information is being collected, used, stored, and sold about them and refuse to provide it. The CCPA will apply specifically to businesses whose annual gross revenues exceed 25 million dollars, technology companies who derive at least 50 percent of their business selling consumer personal information, or sells, receives, or shares the personal information of at least 50,000 consumers, households or devices.

The CCPA’s definition of “personal information” (PI) includes virtually everything. Under the CCPA, “[p]ersonal information’ means information that identifies, relates to, describes, is

\[^{44}\] Tex. Bus. & Com. Code §503.001(c).


\[^{47}\] Id.

capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or device.” For example, PI includes:

- “Biometric information.”
- “Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier Internet Protocol address, email address, account name, social security number, driver’s license number, passport number, or other similar identifiers.”
- “Characteristics of protected classifications under California or federal law.”
- “Commercial information, including records of personal property, products, or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.”

The CCPA creates many new rights for consumers, which in turn creates many new obligations for businesses. The following are the top 11 to keep in mind:

1. “A consumer shall have the right to request that a business that collects personal information about the consumer disclose to the consumer . . . the categories . . . and specific pieces of personal information it has collected about that consumer.”

2. “A business that collects a consumer’s personal information shall, at or before the point of collection, inform consumers as to the categories of personal information to be collected and the purposes for which the categories of personal information shall be used. A business shall not collect additional categories of personal information or use personal information collected for additional purposes without providing the consumer with notice consistent with this section.”

3. “A business that receives a verifiable consumer request from a consumer to access personal information shall promptly take steps to disclose and deliver, free of charge to the consumer, the personal information required by this section. The information may be delivered by mail or electronically, and if provided electronically, the information shall be in a portable and, to the extent technically feasible, in a readily useable format that allows the consumer to transmit this information to another entity without hindrance. A business may provide personal information to a consumer at any time, but shall not be required to provide personal information to a consumer more than twice in a 12-month period.”

4. “A consumer shall have the right to request that a business delete any personal information about the consumer which the business has collected from the consumer.”

5. “A business that collects personal information about consumers shall disclose . . . the consumer’s rights to request the deletion of the consumer’s personal information.”

6. “A consumer shall have the right, at any time, to direct a business that sells personal information about the consumer to third parties not to sell the
consumer’s personal information. This right may be referred to as the right to opt out.”

7. “A third party shall not sell personal information about a consumer that has been sold to the third party by a business unless the consumer has received explicit notice and is provided an opportunity to exercise the right to opt out.”

8. “A business that sells consumers’ personal information to third parties must provide notice to consumers . . . that this information may be sold and that consumers have the right to opt out of the sale of their personal information.”

9. “A business shall not discriminate against a consumer because the consumer exercised any of the consumer’s rights under this title....”

10. “A business shall, in a form that is reasonably accessible to consumers...provide a clear and conspicuous link on the business’ Internet homepage, titled “Do Not Sell My Personal Information,” to an Internet Web page that enables a consumer, or a person authorized by the consumer, to opt out of the sale of the consumer’s personal information. A business shall not require a consumer to create an account in order to direct the business not to sell the consumer’s personal information.”

11. “A consumer may authorize another person solely to opt out of the sale of the consumer’s personal information on the consumer’s behalf, and a business shall comply with an opt out request received from a person authorized by the consumer to act on the consumer’s behalf, pursuant to regulations adopted by the Attorney General.”

Unlike the Illinois law, consumer civil actions are limited to security breaches involving a consumer’s PI. Damages are limited to $750 per consumer per incident or actual damages, whichever is greater. To put it in perspective, a class of 1 million people whose data was compromised would equal $750,000,000 in potential exposure under the CCPA.

Additionally, California law makes it a criminal misdemeanor for employers to share employee fingerprints with "any other employer or third person." Any person who “knowingly causes” the employer to share employee fingerprints with a third party is also guilty of a criminal misdemeanor. Furthermore, the statute provides for treble damages in a civil suit. While it is difficult to imagine this situation arising, they should be mindful that it does not share employee fingerprints with clients or obtain copies of those fingerprints from clients throughout this process.

c. European Union General Data Protection Regulation (GDPR)

As of May 25, 2018, employers must be in full compliance with the GDPR. The GDPR requirements regarding notice, data breach notification, consent, and an individual’s access to data are significantly broader and stricter than the requirements under current national data
protection laws and the EU Data Protection Directive. Additionally, the penalties for noncompliance with the GDPR are severe. Employers that violate the GDPR face fines of 20 million Euros or 4 percent of the company’s worldwide revenue, whichever is greater.

Under the GDPR, biometric information is among the special categories of personal data. As such, processing such data for the purpose of “uniquely identifying a natural person” is prohibited but for a handful of exceptions. Although one such exception is when the individual explicitly consents, employers generally will not be able rely upon an employee’s consent to process the employee’s data because such consent will not be deemed voluntary or freely given because of the unequal bargaining positions between employers and employees. Thus, employers must rely on other, more limited grounds to legally process employee data. Employers with operations in the EU should carefully review any existing or contemplated biometric collection in light of this significant development.

d. Data Breach Notification Laws

Currently only a handful of states regulate the collection of biometric information, but many more states provide protections for personal information and require specific notifications to individuals, often including employees, in the event the security of such information has been compromised. In fact, as of March 1, 2018, only Alabama and South Dakota do not have such laws in place, and both states have bills pending as of the date of publication.52

While many of these laws focus on Social Security Numbers and bank account information, a growing number expressly include biometric information.53

An employer whose principal place of business is in the State of Wisconsin, for example, must make reasonable efforts to notify employees if their personal information is accessed by someone without authorization. According to the statute, “personal information” means an individual’s last name and first name or initial, in combination with any of the following, non-public information that is not encrypted54 or otherwise unreadable:

1. The individual’s Social Security Number.
2. The individual’s driver’s license number or state identification number.
3. The number of the individual’s financial account number, including a credit or debit card account number, or any security code, access code, or password that would permit access to the individual’s financial account.
4. The individual’s deoxyribonucleic acid profile, as defined in s. 939.74(2d)(a).
5. The individual’s unique biometric data, including fingerprint, voice print, retina or iris image, or any other unique physical representation.

54 Under a number of data breach notification laws, including Wisconsin’s, data is not covered personal information if it is encrypted, redacted, or otherwise altered in such a manner that the name or data elements are unreadable unless the keys to unencrypt, unredact, or otherwise read the data have been obtained through a breach of security.
Such notice must be provided within a reasonable time frame, not to exceed 45 days after the employer learns of the unauthorized acquisition of personal information. Although there is no private cause of action to enforce the notice requirements, failure to provide timely notice to affected individuals of a breach involving their personal information can be used as evidence of negligence or a breach of a legal duty.\(^55\)

Iowa’s law is largely similar to the data breach notification requirements in Wisconsin but specifies that notification be provided “immediately” following discovery of the breach.\(^56\) Violations of the data breach notification requirements are considered unlawful practices under Iowa’s Consumer Fraud Statute, which is enforced by the state attorney general.\(^57\) Consequences include damages for injury and a fine of up to $40,000 per violation.\(^58\)

As more and more companies integrate biometrics in their business processes, it is anticipated that the actual text, or judicial interpretations, of data breach notification laws will be modernized to encompass such information within their protections.

e. Accommodation Issues and Potential Discrimination Claims

Employers must also be aware of possible religious objection to the use of biometric information for employment purposes. Title VII of the Civil Rights Act of 1964 (Title VII) makes it an unlawful employment practice “to discharge any individual . . . because of such individual’s . . . religion.”\(^59\) This prohibition includes not making reasonable accommodations for religious observances of employees, absent undue hardship on the employer’s business.\(^60\)

In a recent and well-publicized case, the Fourth Circuit Court of Appeals confirmed that an employee’s firmly held religious beliefs, and by extension, Title VII, can be implicated by use of biometric devices in the workplace.\(^61\) The case involved a mining worker who felt compelled to resign when his employer countermanded his refusal, for religious reasons, to use a newly installed biometric hand scanner to track his time and attendance. In affirming a jury award of $586,861 to the employee, the Fourth Circuit stated that “participating in the hand-scanner system would have presented a threat to [the employee’s] core religious commitments.”\(^62\) More specifically, the employee believed that the hand scanner would imprint him with the “mark of the beast,” which he further believed, based on an interpretation of the biblical Book of Revelation, would permit the Antichrist to manipulate and control his actions.

---

55 Wis. Stat. §134.98(4).
56 Iowa Code §715C.2.2.
57 Iowa Code §715C.2.9.
58 Iowa Code §714.16.7.
60 42 U.S.C. §2000e(j) (defining “religion” to include “all aspects of religious observance and practice, as well as belief,” unless employer can show that accommodation of employee’s religion would impose an “undue hardship on the . . . employer’s business”).
62 Id. at 137.
The EEOC brought suit against the employer, alleging that the employee’s resignation, following on the heels of the employer’s refusal to accommodate his religious beliefs, amounted to an unlawful constructive discharge. After trial, the jury returned a verdict in favor of the EEOC and awarded the employee wages, benefits, and compensatory damages. The jury declined, however, to award punitive damages.

On appeal, the Fourth Circuit agreed that “[t]he evidence presented at trial allowed the jury to conclude that [the employer] failed to make available to a sincere religious objector the same reasonable accommodation it offered other employees, in clear violation of Title VII.”63 In reaching that conclusion, the Court of Appeals confirmed that the proper analysis in such cases is not whether the employee’s belief is correct. To the contrary, the focus should be on whether the belief can be accommodated without an undue hardship on the business. The employer was unsuccessful in the undue hardship argument, in part, because there was evidence that it permitted other employees with hand injuries to manually enter their personnel numbers on a keypad.

Recommended Best Practices

Before collecting, using or storing biometric information, companies should undertake the following actions:

- Review the terms, conditions and capabilities of your biometric equipment and devices. Investigate whether your equipment or devices capture biometric identifiers or biometric information. Understand how the biometric data is captured, encrypted or modified, how and where it is stored and how, when and who destroys it.

- Ensure each employee who uses biometric equipment/devices signs a written policy/consent form that provides the required notice, authorization and written consent (i.e., the purpose for collecting biometric data, all required disclosures including the length of time for which the biometric data is to be collected, stored and used and when it will be destroyed). Post your policies by biometric time clocks, other biometric equipment and employee break areas. Add your retention and destruction schedules to your existing Document Retention Policy or ensure this information is included in your policy/consent form.

- Audit your files periodically to ensure no employees or temporary workers have fallen through the cracks and not received and signed your policy/consent form.

- Request assurances that business partners, temporary staffing agencies, biometric vendors and other third-party vendors comply with applicable biometric and data breach laws. Request written confirmation of their compliance and security protocols. Audit them periodically for compliance.

---

63 Id. at 137.
• If sued, aggressively pursue any and all available insurance. That includes Employment Practices Liability Insurance (EPLI), Cyber insurance and Comprehensive General Liability (CGL) insurance, which generally provides much higher liability limits than EPLI policies. Coverage may exist under the “Personal and Advertising Injury” section of your CGL policy, given Rosenbach’s ruling that BIPA violations cause individuals to suffer a “real and significant” injury to their “right to privacy in and control over their biometric identifiers and biometric information.” Id. at ¶¶33-34.

• Review contracts with business partners, temporary staffing agencies and biometric and other third-party vendors to understand indemnification, hold harmless and cost of defense rights and responsibilities, if any.

• Understand and comply with applicable data breach notification requirements.

• Ensure you provide for religious and disability-based accommodations, when necessary.

Microchipping and Wearables—Recommended Best Practices

• In general, give employees the ability to choose whether to implant microchips or use wearable technology, document that choice and their decision in writing.

• Check your state’s laws regarding microchipping. Be sure to obtain an employee’s written consent before implanting a microchip.

• Regardless of whether you must obtain consent to microchip employees, be sure to inform employees of what data the microchip obtains from them so as not to trigger liability under other, secondary laws.

• Only monitor for legitimate business reasons, such as accessing company property or information.

• Safeguard data privacy by, at a minimum, encrypting the data collected. If data is not technically encrypted, ensure it is modified to be unidentifiable or unrecognizable.
Biometrics and Beyond: The Evolution of Workplace Privacy Issues

Presenters
Wes Carlisle (Dhanani Group), Keith E. Kopplin (Milwaukee), and Anne E. Larson (Chicago)

Moderator
Wade M. Fricke (Cleveland)

Roadmap of Discussion

- Benefits and Risks of:
  - Microchipping
  - Wearables
  - Biometric Equipment
- Biometric Information Protection Act, Other State Biometric Laws, and EU GDPR
- BIPA Class Actions – over 220 filed
- Data Breach Notification Laws
- Best Practices
What is Microchipping?

Benefits of Microchipping

- Easier access to company facilities and devices
- More secure access to facilities and devices
- Less cumbersome and more accurate timekeeping
- Facilitate sales transactions
- An opportunity to be at the forefront of technology
Risks of Microchipping

- State laws – regulation and compliance
- Workers’ compensation claims
- Accommodation requests – religious and disability
- Privacy concerns
What are Wearables?

- Types:
  - Wristbands
  - Modular sensors
  - “Smart” hats
  - Clothing
  - Eyewear
  - Ear wear

Benefits of Wearables

- Employee wellness
- Workplace safety
- Efficiency/productivity
- Connectivity
Risks of Wearables

- Unwanted discoveries/revelations
- Invasion of privacy
- Data security
- Employee morale
- Device abandonment
What are Biometrics?

- Definition: “the measurement and analysis of unique physical and behavioral characteristics (such as fingerprint or voice patterns) especially as a means of verifying personal identity.”
- Examples: fingerprint, palm print, voice print, DNA, scans of retina, iris and facial geometry, gait analysis, and odor/scent

Benefits of Biometrics

- Fulfill timekeeping obligations
- Detect and reduce employee fraud
- Increase productivity
- Manage workflow/increase efficiency
- Minimize leave abuse
- Control access to facilities and equipment
- Process transactions
Risks of Biometrics

- BIPA class actions – $1,000 or $5,000 for “each violation”
- Texas and Washington Attorney General actions
- Data breach notification laws – in 48 states
- California CPL – class action potential with $750 in damages per consumer per incident for security breaches involving biometric data; misdemeanor
- European Union Data Privacy Regulation
- Disability or religious discrimination claims

Biometric Information Privacy Act

- **Enacted** in 2008; over 220 class actions
- **Biometric identifier**: fingerprint, voiceprint and scan of retina, iris, hand or face geometry
- **Biometric information**: any information, regardless of how it is captured, converted, stored, or shared, based on an individual’s biometric identifier used to identify an individual
**BIPA Compliance Obligations**

- Company may not collect biometric data **unless** it first:
  - Informs the individual in writing that a biometric identifier or biometric information is being collected or stored;
  - Informs the individual in writing of the specific purpose and length of term for which a biometric identifier or biometric information is being collected, stored, and used; and
  - Obtains written consent from the individual.

**Rosenbach Ruling and Defenses**

- *Rosenbach* – Ill. Supreme Court (Jan. 25, 2019)
- Defense Arguments
  - Preempted by exclusive remedy provisions of Workers’ Compensation Act
  - Barred by applicable Statute of Limitations (SOL)
    - 1-yr SOL for Privacy Violations
    - 2-yr SOL for Negligence or Statutory Penalties
    - 5-yr Catch-all SOL
  - Implied Consent
Open Issues

- What does “each violation” mean?
- Potential transfer of millions to plaintiffs’ class action bar
- Insurance coverage concerns
- BIPA fails to account for biometric technology that protects biometric data. Compare data breach statute – Wis. Stat. §134.98(1)(b)
- Lobbying efforts to amend BIPA

Best Practices

- Regularly audit compliance with biometric and data breach laws – your company’s and vendor’s
- Understand how biometric data is captured and modified, who stores it, and who destroys it
- Review contracts with business partners/vendors
- Tender claims to Cyber, EPLI, and GCL policies
- Provide reasonable accommodations
- Safeguard data privacy; prepare for breaches
- Stay tuned for more legislation!
Biometrics and Beyond: The Evolution of Workplace Privacy Issues

Presenters
Wes Carlisle (Dhanani Group), Keith E. Kopplin (Milwaukee), and Anne E. Larson (Chicago)

Moderator
Wade M. Fricke (Cleveland)