ALFA International
THE GLOBAL LEGAL NETWORK

2024 Hospitality & Retail Practice Group Seminar

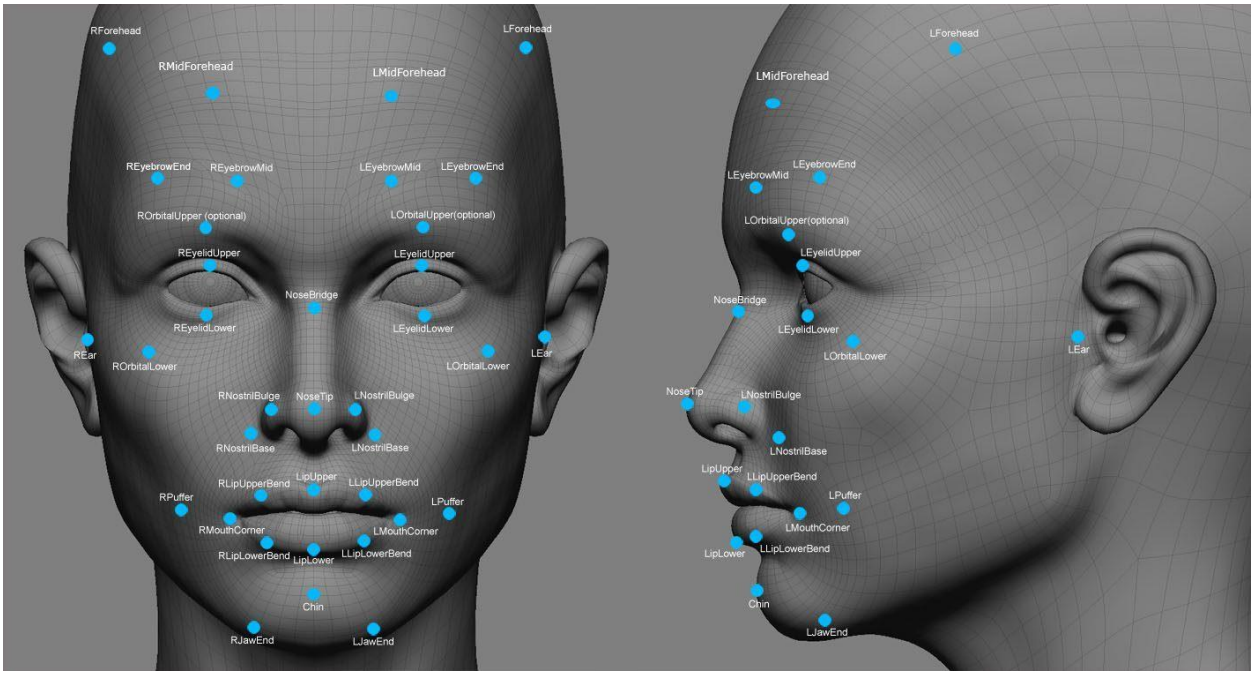
May 29-31, 2024

Weighing the Risks and Benefits of Artificial Intelligence in Hospitality and Retail—Who Wins—Man, Machine, or Both?

Allen Sydnor
Moderator
HUIE, FERNAMBUCQ & STEWART LLP
Birmingham, Alabama
asydnor@huielaw.com

"Sometimes you want to go where everybody knows your name"

(just not everything else about you)



Introduction

Every retailer, restaurant, and hotel would love to develop the type of customer loyalty embodied in the theme from the long-running show *Cheers.* Predictions are Artificial Intelligence (AI)[i] will aid that goal.[ii] However, surveys reflect customers generally do not trust that the privacy of their personal information will be maintained[iii] and if they read the "Privacy Notice" or the "Cookie Notice" on the websites of their favorite retailer, hotel, or restaurant it would confirm their suspicions. The industry itself recognizes that privacy along with cybersecurity is one of the biggest potential risks associated with AI use,[iv] but a risk that it must learn to understand and manage rather than ignore the potential positive impact AI can have on their growth. Potential future litigation is often foretold by examination of prior and pending cases. In the hospitality and retail industry, use of session replay software on websites and use of biometrics has been the genesis of most breach of privacy litigation. This paper is intended to identify exemplary cases and provide an overview of the claims and issues the growing use of AI is likely to spawn.

Current Legislative Landscape

Although the FTC issued a policy statement on the use of biometrics in May 2023[v] and President Biden signed an Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence in October 2023,[vi] Congress has failed to adopt uniform laws regulating use of AI. However, privacy is a global concern, at least in countries with democratic forms of government. A number of countries, as well as some State Legislatures, have looked to the European Union's General Data Protection Regulation ("GDPR") as a model for protecting the privacy of their citizens. It imposes strict limitations on the processing of biometric data. Entities with an international footprint are looking at conformance with the GDPR as the safest path.[vii] The absence of uniform federal law in the U.S. means businesses are subject to state privacy laws that vary in definitions and forms of compliance.

Consequently, civil litigation in the United States has been premised primarily on statutes in four states - California[viii], Florida[ix], Illinois[x], and Pennsylvania[xi]. Although many other states have privacy laws, most specifically bar private causes of action and leave enforcement up to State authorities.[xii] That means State Attorney Generals have the authority to file enforcement actions[xiii] similar to the ones pursued in Texas against Meta (Facebook) and Google which represent potential exposure of $25,000 for each noncompliant capture of a biometric identifier.[xiv] The potential financial impact of complying with 50 distinct state laws has been estimated to "surpass $1 trillion over a decade."[xv]

In December 2023, the federal government flexed its muscles with the Federal Trade Commission entering into a settlement with Rite Aid banning the pharmacy chain from using facial recognition technology for the next five years. The action was taken based on charges that the company misused AI biometric surveillance technology in hundreds of its stores to identify customers who have engaged in shoplifting and other problematic behavior in its stores.[xvi] The proposed order prohibits Rite Aid from misrepresenting its data security and privacy practices and also require the company to:

- **Delete, and direct third parties to delete**, any images or photos they collected because of Rite Aid's facial recognition system as well as any algorithms or other products that were developed using those images and photos.
- **Notify consumers** when their biometric information is enrolled in a database used in connection with a biometric security or surveillance system and when Rite Aid takes some kind of action against them based on an output generated by such a system.
- **Investigate and respond** in writing to consumer complaints about actions taken against consumers related to an automated biometric security or surveillance system.
- **Provide clear and conspicuous notice** to consumers about the use of facial recognition or other biometric surveillance technology in its stores.
- **Delete any biometric information** it collects within five years.
- **Implement a data security program** to protect and secure personal information it collects, stores, and shares with its vendors.
- **Obtain independent third-party assessments** of its information security program; and
- **Provide the Commission with an annual certification** from its CEO documenting Rite Aid's adherence to the order's provisions.

Biometrics lawsuits have resulted in multi-million dollar judgments or settlements[xvii], whereas Defendants have usually prevailed in the website session replay lawsuits. However, few major retailers have escaped getting named in these lawsuits and there are appeals pending that could change the landscape of expectations about results.[xviii]

Understanding the Technology at the Core of the Litigation

To defend any litigation, both in-house and outside counsel need to have a basic understanding of what the software and/or technology involved actually do that gives rise to the claims. Some reported cases include explanations.

Session Replay Software Litigation

Much of the litigation relying on privacy laws as a basis of their claims has arisen from the use of some form of session replay software. Although most of these lawsuits do not involve true AI versions, they can fairly be viewed as the basic roadmap Plaintiff's attorneys will use as companies convert to the AI enhanced versions of session replay software. In fact, Microsoft's current version of Clarity is Clarity AI.

The most frequently reported session replay lawsuits involve the use of session software such as Microsoft's Clarity, Quantum Metric or Mouseflow. Two exemplary cases that provide helpful "tutorials" about the software and how their use is the basis of Plaintiffs' claims are *Price v. Carnival Corp*.[xix] and *In re BPS Direct*.[xx] In *Price,* Plaintiffs alleged that Carnival Cruise Lines used the Clarity software on its website to intercept Plaintiffs' personal information, including their "passport number, driver's license number, date of birth, home address, phone number, email address and/or payment information," and used that information to trace their browsing history on other sites in violation of Federal and State laws.[xxi]. Before ruling on Carnival's Motion to Dismiss, the Court explained how the Clarity software works:

Microsoft calls its Session Replay Code "Clarity" and embeds Clarity on Carnival's "website, either by directly hard-coding the code on the website or through a third-party platform . . . ." When a user visits the website, Clarity is "deploy[ed]" onto the user's browser. There, it collects information about the user's system, including their device, browser, operating system, and location, as well as "all mouse movements, clicks, scrolls, zooms, window resizes, keystrokes, text entry (even if deleted), and numerous other forms of a user's navigation and interaction through the website." Clarity transmits the collected information to Microsoft's server in "hyper-frequent logs" which are "often just milliseconds apart."

After recording the user's information, Microsoft "analyze[s]" it. ("Both Carnival and the Session Replay Providers access and analyze the video replay of the user's behavior on the website."). Microsoft provides Carnival with a reenactment of the user's visit, akin to "a video replay," and uses Clarity to create "detailed heatmaps" for Carnival, "that provide information about which elements of a website have high user engagement." Clarity's most powerful function, however, is its ability to expose a user's browsing on other sites. Clarity attaches a "specific user ID," or a "fingerprint," to a visitor's profile based upon their unique "combination of computer and browser settings, screen configuration, and other detectable information." Carnival accesses these fingerprints, which are collected across every site that Clarity is deployed on and uses them to link a user's session to "web browsing across other websites previously visited, including on websites where the user had intended to remain anonymous." Plaintiffs allege that Carnival uses Microsoft's services to create "unique IDS and profiles" for each of its users, "de-anonymizing" its users' internet browsing.

Defenses and Outcomes

The outcomes of most cases have been dictated by the application of well-established legal principles such as lack of standing or failure to plausibly state a claim. Many have been dismissed because Plaintiffs have failed to demonstrate the "real," "concrete injury" required by *Spokeo v. Robins*, 136 S. Ct. 1540 (2016). Such was the case in *Popa v PSP*[xxii] currently pending in the 9th Circuit for review of the dismissal of Plaintiff's complaint. Plaintiff claims that she adequately demonstrated her Article III standing when she alleged that the Session Replay Code intercepted and disclosed her private online communications without her knowledge or consent, in violation of the Pennsylvania anti-wiretapping statute. Briefing in that case is not scheduled to be completed until June 2024.

Biometric Litigation

Biometric authentication involves using some part of your physical makeup to authenticate you. This could be a

fingerprint, an iris scan, a retina scan, or some other physical characteristic. A single characteristic or multiple characteristics could be used. According to a 2022 survey by the National Retail Federation and Loss Prevention Research Council, 12.3% of respondents were implementing or planning to implement facial recognition for loss prevention.[xxiii] Others, like Amazon are aggressively proceeding forward with the use of biometric payment systems. In 2023 Amazon announced a rollout of its palm recognition biometric authentication service, Amazon One, within 500 Whole Foods and Amazon Fresh locations across the U.S.

Most of the biometric litigation arises from alleged violations of the Illinois Biometric Information Privacy Act BIPA. BIPA regulates private entities or "any individual, partnership, corporation, limited liability company, association, or other group, however organized."[xxiv] BIPA's definition of "biometric identifier" includes "a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry."[xxv] It has been reported that in the last few years, more than 200 companies across a range of industries (from locker rental companies to tanning salons) have been sued for allegedly violating BIPA.[xxvi] Facebook agreed to pay $650 million in 2021 to settle a class action lawsuit alleging that the app violated the state's biometric privacy law by using facial recognition technology until November 2021. In similar lawsuits, Google agreed to pay $100 million, TikTok $92 million, and Snapchat $35 million.

Lawsuits range from suits by employees and vendors required to clock in with their thumbprints to claims by consumers against major retailers and device manufactures like Apple who use facial recognition software. Although the law was enacted in 2008, it was not until the Illinois Supreme Court held in *Cothron v. White Castle* that BIPA violations accrue each time a private company scans a person's biometric identifier that class actions took off as a means of recovery. Other important decisions paving the way for a multitude of lawsuits were *Rosenbach v. Six Flags Entertainment Corp* and *Patel v. Facebook*. The court in *Rosenbach v. Six Flags* held:

1) BIPA "codified that individuals possess a right to privacy in and control over their biometric identifiers and biometric information."

2) Violations are not "merely 'technical' in nature" because "an individual's unique biometric identifiers . . . cannot be changed if compromised or misused."

3) "[A]n 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."

In *Patel,* the court held that the violation of BIPA's notice and consent provisions amounts to a concrete injury-in-fact (not merely a procedural violation) sufficient to confer Article III standing to plaintiffs. In *Tims v. Black Horse Carriers Inc.*, 2023 IL 127801, the Illinois Supreme Court held that all claims under BIPA are subject to a five-year statute of limitations.

Examples of the type of litigation under BIPA include:

- Claims that Amazon sells its Rekognition technology, which analyzes biometric identifiers to increase its accuracy, to various organizations.[xxvii]

- Claims that HireVue, Inc. violated BIPA when its interactive software captured and collected their biometric information during virtual job interviews.[xxviii]

- Claims that Apple profited "through marketing and selling its devices based upon claims of photograph sorting technology."[xxix]

- Claim that McAlister's Deli and Focus Brands required a franchisee, Aggressive Developments, to have its employees, clock in and out of work using their fingerprints and "collected, stored, and used Plaintiff's biometrics" without providing written disclosures or obtaining Plaintiff's consent.[xxx]

- Claim that Macy's purchased access to the Clearview database and the biometrics contained therein to identify people whose images appeared in surveillance camera footage from Macy's retail stores. Plaintiffs asserted that Macy's utilized Clearview's database over 6,000 times, each time uploading an image to the database to search for a match.[xxxi]

- Claim against Marriott by employee where Marriot required its employees to register and scan their fingerprint for timekeeping purposes each time they clocked-in and out at work. To accomplish this, Chicago Marriot hired Paychex, a prominent biometric timekeeping provider in Illinois, to collect and store its employee's biometric data. Paychex hosts a variety of cloud-based apps supported by and stored on Microsoft's Azure platform.[xxxii]

- Claim by mother for minor child alleging Players of NBA 2K, such as Plaintiff's minor child, take and scan multiple photos of their faces on the Take 2 app and upload those images to the AWS/Amazon cloud to make customized players resembling the user.[xxxiii]

Target is one of the latest to be sued. A recent lawsuit alleges that Target uses a network of more than a dozen "investigation centers" along with a pair of forensic labs where video footage is allegedly enhanced and fingerprints are analyzed. The filing acknowledges that the system was used with the intent of detecting shoplifters and preventing theft, but states that the system also managed to capture the facial biometric data of all customers every time they entered or exited Target property.[xxxiv]

Insurance Coverage for Biometric Lawsuits

As expected, challenges to coverage are not far behind the filing of lawsuits. In *National Fire Ins. Co. of Hartford* and *Continental Ins. Co. v Visual Pak Company, Inc.*,[xxxv] the Court held that the two companies did not have a duty to defend a claim brought under BIPA wherein the Plaintiff claimed he had been forced to enroll in an employee database using a fingerprint scan. In *Thermoflex Waukegan, LLC v. Mitsui Sumitomo Ins. USA, Inc*., 2023 U.S. Dist. LEXIS 9282 (N.D. Ill. 2023), the Court held certain policy provisions to be too ambiguous thus requiring coverage while finding no coverage under another provision. *W. Bend Mut. Ins. Co. v. Krishna Schaumburg Tan, Inc*. broadened insurance liability holding that a Commercial general liability insurance for personal injury potentially covers BIPA lawsuits. Thus, the expectation is that insureds and insurers will likely continue to litigate coverage as they both attempt to control the expense of litigating breach of privacy claims related to use of biometrics.

Evidentiary Issues Related to Artificial Intelligence

One of the questions that has been posed is how to treat AI in legal proceedings. Should evidence gleaned from AI be judged by the standard of direct witness testimony, expert witness testimony, or measured by standards for technology. [xxxvi] In *State v. Morrill*,[xxxvii] a criminal defendant challenged reliability and raised hearsay objections with respect to automated conclusions from Roundup and Forensic Toolkit, two AI assisted analytical programs used by the prosecution. After a two day Daubert hearing, the court deemed the software reliable and declined to consider it hearsay because the hearsay rules defined a "[d]eclarant" as "the person who made the statement" and a "[s]tatement" as "a person's oral assertion, written assertion, or nonverbal conduct, if the person intended it as an assertion." Since the software was not a "person," the rule did not bar the evidence as hearsay.

In *Bertuccelli v. Universal City Studios LLC*, No. 19-1304, Order (E.D. La. Oct. 21, 2020), the court recognized the reliability of an expert's methodology "given that he conducted an artificial intelligence assisted facial recognition analysis of [the masks at issue] to determine whether the use of mathematics and target facial recognition algorithms comparing the two works would find that human perception would view the works to be substantially similar."

As a general reference on this subject see Artificial Intelligence and the Courts: MATERIALS FOR JUDGES.[xxxviii]

Conclusion

Changes in technology test the sufficiency of existing laws and can result in attempts to apply them in ways never anticipated. AI is one of those areas where legislators, regulators, and courts are struggling to keep up and adjust. As noted by the Court in *Goldstein v. Costco Wholesale Corp*.[xxxix]:

Courts bear the responsibility of applying the law to a constantly shifting technological and societal landscape. When the Framers crafted the Fourth Amendment to the United States Constitution, for example, they could not have envisioned how smartphones and GPS would fit into the framework of "papers" and "effects." … But the courts' flexibility has its limits. Courts may not rewrite statutes to change with the times. The Constitutions of Florida and the United States give this power to the legislative bodies alone. Rather, the Court must take the law as it is and apply it faithfully to new facts as they arise.

---

[i] Artificial Intelligence has been defined as the hypothetical ability of a computer to match or exceed a human's performance in tasks requiring cognitive abilities, such as perception, language understanding and synthesis, reasoning, creativity, and emotion. See, See A.M. Turing, I.—Computing Machinery and Intelligence, 59 MIND 433, 460 (1950); John McCarthy et al., A Proposal for the Dartmouth Summer Research Project on Artificial Intelligence, August 31, 1955, reprinted in 27 AI MAG. 12 (2006).

[ii] Here's how artificial intelligence can benefit the retail sector https://www.weforum.org/agenda/2023/01/here-s-how-artificial-intelligence-benefit-retail-sector-davos2023/; AI In Hospitality: Elevating The Hotel Guest Experience Through Innovation https://www.forbes.com/sites/neilsahota/2024/03/06/ai-in-hospitality-elevating-the-hotel-guest-experience-through-innovation/?sh=44e7901377d4

[iii] 64 Alarming Data Privacy Statistics Businesses Must See in 2024, https://termly.io/resources/articles/data-privacy-statistics/

[iv] Risk Mitigation Strategies for Retailers Rolling Out AI Solutions, https://www.bdo.com/insights/industries/retail-consumer-products/risk-mitigation-strategies-for-retailers-rolling-out-ai-solutions#:~:text=Some%20of%20the%20main%20challenges,on%20their%20rights%20and%20dignity.

[v] https://www.ftc.gov/news-events/news/press-releases/2023/05/ftc-warns-about-misuses-biometric-information-harm-consumers

[vi] https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

[vii] https://www.techtarget.com/searchdatabackup/tip/6-business-benefits-of-data-protection-and-GDPR-compliance

[viii] California: California Invasion of Privacy Act ("CIPA"), Cal. Penal Code §§ 631 & 632;

[ix] Florida: Florida Security of Communications Act ("FSCA") The FSCA, provides a cause of action against parties that intercept or use private communications without the speaker's consent. Fla. Stat. §§ 934.10(1)(a), (d).

[x] Illinois: The Biometric Information Privacy Act (BIPA) (740 ILCS 14/15(b), (d) The Act provides that a private entity may not "collect, capture, purchase, receive through trade, or otherwise obtain" a person's biometric data without first providing notice to and receiving consent from the person. 740 ILCS 14/15(b) (West 2018). Section 15(d) provides that a private entity may not "disclose, redisclose, or otherwise disseminate" biometric data without consent. Id. § 15(d). Under BIPA " any person 'aggrieved' by a violation of its provisions 'shall have a right of action against an offending party' and 'may recover for each violation.

[xi] Pennsylvania: Pennsylvania Wiretapping and Electronic Surveillance Control Act,(WESA) 18 Pa. Cons. Stat. § 5701 et seq.,

[xii] https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2021/06/Biometric-Privacy-Fact-Sheet.pdf The State of Privacy, How state "privacy" laws fail to protect privacy and what they can do better , https://epic.org/wp-content/uploads/2024/01/EPIC-USPIRG-State-of-Privacy.pdf

[xiii] US State Privacy Legislation Tracker https://iapp.org/resources/article/us-state-privacy-legislation-tracker/

[xiv] See, https://www.courthousenews.com/wp-content/uploads/2022/10/texas-lawsuit-against-google-in-midland-county-district-court.pdf; https://texasattorneygeneral.gov/sites/default/files/images/child-support/State%20of%20Texas%20v.%20Meta%20Platforms%20Inc..pdf

[xv] Jennifer Huddleston and Gent Salihu "The Patchwork Strikes Back: State Data Privacy Laws after the 2022–2023 Legislative Session" https://www.cato.org/blog/patchwork-strikes-back-state-data-privacy-laws-after-2022-2023-legislative-session-0

[xvi] Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards, https://www.ftc.gov/news-events/news/press-releases/2023/12/rite-aid-banned-using-ai-facial-recognition-after-ftc-says-retailer-deployed-technology-without

[xvii] See e.g., Rogers v. BNSF Ry. Co., No. 19 C 3083, 2023 U.S. Dist. LEXIS 113278, 2023 WL 4297654, at *6 (N.D. Ill. June 30, 2023)($228 million jury verdict—45,600 BIPA violations multiplied by $5,000 per violation in class action for truck drivers who were required to scan a biometric identifier into identity verification devices to enter BNSF railyards.)
[xviii] Popa v. PSP Grp. LLC, 2023 U.S. Dist. LEXIS 210520 *; 2023 WL 8188726 (W.D. Wash. 2023)
[xix] 2024 U.S. Dist. LEXIS 10175 *; 2024 WL 221437 (S.D. Cal. 2024)
[xx] In re BPS Direct, LLC, No. 22-CV-4709, 2023 U.S. Dist. LEXIS 216728, 2023 WL 8458245, at *13 (E.D. Pa. Dec. 5, 2023)
[xxi] Federal Wiretap Act, 18 U.S.C. § 2510, et seq., the Computer Fraud and Abuse Act, 18 U.S.C. §1030, the California Invasion of Privacy Act ("CIPA"), Cal. Penal Code § 630, et seq., the Maryland Wiretapping and Electronic Surveillance Act, Md. Code Ann., Cts. & Jud. Proc. § 10-401, et seq., the Massachusetts Wiretap Act, Mass. Gen. Laws ch. 272, §99, the Pennsylvania Wiretapping and Electronic Surveillance Control Act, 18 Pa. Cons. Stat. § 5701 et seq
[xxii] 2023 U.S. Dist. LEXIS 210520 *; 2023 WL 8188726 (W.D. Wash. 2023)
[xxiii] See, e.g., National Retail Federation and Loss Prevention Research Council, 2022 Retail Security Survey: The State of National Retail Security and Organized Retail Crime, 17, https://nrf.com/research/national-retail-securitysurvey-2022
[xxiv] See 740 ILL. COMP. STAT. §§ 14/10-20
[xxv] 740 ILL. COMP. STAT. § 14/10.
[xxvi] https://law.siu.edu/_common/documents/law-journal/articles-2019/summer-2019/8-insler-jr-final.pdf
[xxvii] Hogan v. Amazon.com, Inc., No. 21 C 3169, 2022 U.S. Dist. LEXIS 58347, 2022 WL 952763, at *7 (N.D. Ill. Mar. 30, 2022)
[xxviii] Deyerler v. HireVue, Inc., No. 22 CV 1284, 2024 U.S. Dist. LEXIS 32211, 2024 WL 774833, at *6 (N.D. Ill. Feb. 26, 2024)
[xxix] Hazlitt v. Apple Inc., 543 F. Supp. 3d 643, 647 (S.D. Ill. 2021)
[xxx] Rushing v. McAlister's Franchisor SPV LLC, 2023 U.S. Dist. LEXIS 29555 ( )
[xxxi] In re Clearview AI, Inc., 2022 U.S. Dist. LEXIS 14882 *; 2022 WL 252702 (N.D. Ill. 2022)
[xxxii] Jones v. Microsoft Corp., 649 F. Supp. 3d 679 (N.D. Ill. 2023)
[xxxiii] Mayhall v. Amazon Web Servs., Inc., 2023 U.S. Dist. LEXIS 57070 (W.D. Wash. 2023)
[xxxiv] BIPA Lawsuit Takes Aim at Target https://findbiometrics.com/bipa-lawsuit-takes-aim-at-target/
[xxxv] 2023 IL App (1st) 221160
[xxxvi] Paul W. Grimm, Maura R. Grossman, and Gordon V. Cormack, Artificial Intelligence as Evidence, 19 NW. J. TECH. & INTELL. PROP. 9 (2021).
[xxxvii] 2019 N.M. App. Unpub. LEXIS 255 (N.M. App. 2019
[xxxviii] https://www.aaas.org/sites/default/files/2022-09/Paper%202_AI%20and%20Trustworthiness_NIST_FINAL.pdf?adobe_mc=MCMID%3D52000637841860946489208149054056839995%7CMCORGID%3D242B6472541199F70A4C98A6%2540AdobeOrg%7CTS%3D1679961600
[xxxix] 559 F. Supp. 3d 1318 *; 2021 U.S. Dist. LEXIS 170815 **; 2021 WL 4134774 (S.D. Fla. 2021)