SQUIRE PATTON BOGGS

2022 Q3 AI/Biometric Privacy Quarterly Review

US – November 2022

Welcome to the 2022 Q3 edition of the *Artificial Intelligence & Biometric Privacy Report*, your go-to source for keeping you in the know on all recent major artificial intelligence ("AI") and biometric privacy developments that have taken place over the course of the last three months. We invite you to share this resource with your colleagues and visit Squire Patton Boggs' Data Privacy, Cybersecurity & Digital Assets and Privacy & Data Breach Litigation homepages for more information about our capabilities and team. And if you are not currently subscribed to our leading *Consumer Privacy World* blog, make sure to do that by clicking here.

Also, we are extremely pleased to announce that our own Kristin Bryan was named as a 2022 *Law360* Cybersecurity & Privacy MVP. As *Law360* notes, "[t]he attorneys chosen as *Law360*'s 2022 MVPs have distinguished themselves from their peers by securing hard-earned successes in high-stakes litigation, complex global matters and record-breaking deals." You can read more about Kristin's *Law360* award here: Law360 MVP Awards Go to 188 Attorneys From 78 Firms.

New and Emerging Trends

Discrimination and Bias Issues Relating to AI Consumer Tools in Crosshairs of Federal Trade Commission and Consumer Financial Protection Bureau

Today, AI continues to offer companies a myriad of benefits when used in commercial operations – including increased efficiency, reduced costs, enhanced customer experiences, and smarter decision-making, among others. At the same time, however, growing reliance on these tools has also garnered increased interest from lawmakers and regulators concerned about potential fairness and bias issues associated with the use of this technology. In June 2022, the Federal Trade Commission ("FTC") issued its *Combatting Online Harms Through Innovation: A Report to Congress*, in which the agency signaled its positions on AI and intent to enhance its enforcement efforts in connection with improper uses of algorithmic decision-making tools. More recently, on August 11, 2022, the FTC reemphasized the priority focus it has placed on policing AI with the issuance of its Advanced Notice of Proposed Rulemaking on commercial surveillance and lax data security practices ("Commercial Surveillance ANPR"), a large portion of which focuses on issues relating to AI and whether the FTC should promulgate new rules to regulate or otherwise or otherwise limit the use of these advanced technologies. At the same time, the Consumer Financial Protection Bureau ("CFPB") also recently released its *Circular 2022-03: Adverse Action Notification Requirements in Connection With Credit Decisions Based on Complex Algorithms*, which cautions creditors of the need for compliance with the Equal Credit Opportunity Act ("ECOA") when making credit decisions with the aid of complex algorithms.

Takeaways: Taken together, companies should take note of this new federal regulatory agency focus on closely scrutinizing the use of consumer AI tools, especially as it relates to their potential discriminatory impact on protected classes, and ensure that their AI practices are in full compliance with the law to manage associated legal risks.

Additional Reading: For more information and analysis on the FTC's *Combatting Online Harms* Report, please see our *Consumer Privacy World* blog post authored by our team members Kristin Bryan, Kyle Fath, and David Oberly here: FTC Signals Intent to Begin Rulemaking on Privacy and AI, Hints at Areas of AI Focus in Congressional Report.

Additional Reading: For more information and analysis on the FTC's Commercial Surveillance ANPR, please see our *Consumer Privacy World* blog post authored by our team members Kristin Bryan and Kyle Fath here: FTC Issues Advanced Notice of Public Rulemaking for Privacy Regulations.

Discrimination and Bias Issues Relating to AI Hiring/Employment Tools are a Growing Concern of the US Equal Employment Opportunity Commission

The US Equal Employment Opportunity Commission ("EEOC") has also signaled its intent to closely scrutinize the use of AI tools in hiring and employment decisions to ensure that employers and vendors use these technologies fairly and consistently with federal equal employment opportunity laws. In May, the EEOC issued *The Americans With Disabilities Act and the Use of Software, Algorithms, and Artificial Intelligence to Assess Job Applicants and Employees* – extensive guidance designed to assist employers in avoiding violations of the Americans With Disabilities Act ("ADA") when using AI to assess job candidates and employees. The EEOC guidance provides a detailed discussion of the primary ways in which the use of AI tools can result in disability discrimination while also offering several "promising practices" that employers can implement to comply with the ADA when leveraging the benefits of AI technologies. Of note, within just a few days of issuing its guidance, the EEOC filed a federal age discrimination suit against a software developer alleging that its application software engaged in intentional discrimination in violation of the Age Discrimination in Employment Act ("ADEA") through programming that solicited birthdates and automatically rejected applicants based on their age.

Takeaways: Moving forward, employers should anticipate that the EEOC will maintain its focus on increasing its enforcement efforts in this space for the foreseeable future, especially as reliance on algorithmic decision-making tools continues to expand at a rapid clip. In the interim, companies that utilize AI in their hiring and employment decisions – or intend to do so in the future – should take proactive measures by modifying or enhancing their compliance programs to ensure they adequately address the issues outlined in the EEOC's AI ADA guidance.

Additional Reading: For more information on the EEOC's new ADA guidance, read our team member David Oberly's *American Bar Association Cybersecurity & Data Privacy Committee Newsletter* article here: Takeaways From EEOC Guidance on Use of AI in Hiring & Employment Decisions.

Retailers Continue to Be Prime Target for Range of Biometric Information Privacy Act Class Action Suits

As has been the case for well over a year now, one of the largest recent trends in Biometric Information Privacy Act ("BIPA") litigation that continued over the course of 2022 Q3 was the targeting of online retailers in class action lawsuits alleging violations of Illinois's biometric privacy statute. Generally speaking, this can be attributed to (among other factors) retailers' extensive use of technology that at least allegedly appears (according to the plaintiff's counsel) to implicate facial recognition and the availability of liquidated damages on a per violation basis under BIPA. For example, in two currently pending class actions, a proprietary technology platform company was sued for alleged BIPA violations in connection with its "Smart Coolers" technology, which displays targeted advertisements on digital screens in retail store refrigerator cases based on a customer's age, gender, and emotional disposition. In those cases, the plaintiffs allege that the company's technology monitors shoppers using customer detection analysis to interpret collected data using a "facial profiling system" and, in turn, ascertain an individual's "age, gender and emotional response." In addition, retailers have also faced a high volume of BIPA lawsuits in connection with their use of virtual try-on ("VTO") tools, which utilize facial feature detection capabilities to allow users to virtually "try on" products, such as eyewear or cosmetics, to see how they might look on them prior to making a purchase by virtually placing the product on the user's face. Importantly, despite the questionable nature of merits of the claims underlying these lawsuits, *i.e.*, whether the VTO tools in question engage in scans of face geometry, the majority of defendants in these class actions have been unable to obtain dismissals at the motion to dismiss stage. Retailers are also being targeted for BIPA class lawsuits in a broad range of other contexts, such as the use of AI voice assistants that facilitate customers' drive-thru orders, as well as restaurants' use of automated voice order ("AVO") systems that enable customers to place orders over the phone.

Takeaways: If they have not already done so, all retailers should consult with experienced biometric privacy counsel to review their current practices relating to the collection and use of biometric data and remediate any compliance gaps immediately.

Additional Reading: For more information on this hot-button topic, read the highlights from our team member David Oberly's interview with *Bloomberg Law* here: As Virtual Try-On Fashion Technology Grows, So Do Legal Risks.

Broader Interpretation of BIPA Section 15(c) Profiting Claims

Until recently, courts had interpreted BIPA Section 15(c) profiting claims in a relatively narrow fashion, finding that "unlawful sales or profiting" claims under Section 15(c) could exist only where: (1) biometric data is directly sold; (2) actual biometric data is disseminated or access to such data shared; or (3) the technology at issue is so intertwined with the biometric data that by marketing its product, the defendant is essentially disseminating the biometric data for profit. *See Flores v. Motorola Solutions, Inc.*, No. 20 CV 1128, 2021 U.S. Dist. LEXIS 21937, at *5-6 (N.D. Ill. Jan. 8, 2022); *Vance v. Microsoft Corp.*, 534 F. Supp. 3d 1301, 1307-09 (W.D. Wash. 2021). In the recent opinion in *Karling v. Samsara, Inc.*, No. 22 CV 295, 2022 U.S. Dist. LEXIS 121318, at *18-19 (N.D. Ill. July 11, 2022), however, the court interpreted Section 15(c) in a much more expansive fashion, holding that allegations that "profit[ing] from contracts to capture [biometric] data and provide services [utilizing that data] to employers" was sufficient to avoid dismissal of a Section 15(c) claim under Federal Civil Rule 12(b)(6). Similarly, in *Mahmood v. Berbix, Inc.*, No. 22 CV 2456, 2022 U.S. Dist. LEXIS 153010, at *6-7 (N.D. Ill. Aug. 25, 2022), the court held that a plaintiff plausibly alleged that a defendant violated Section 15(c) merely by setting forth allegations that the defendant's customer paid for access to its facial recognition platform to verify the plaintiff's age and identity before she rented a car. Notably, the *Berbix* court reasoned that "[i]n short, [the defendant's] collection and use of biometrics is a necessary component to its business model," which the court found satisfied the standard for plausibly alleging an unlawful sales or profiting claim under Illinois's biometric privacy statute – a looser standard for Section 15(c) claims as compared to earlier BIPA opinions.

Takeaways: As courts begin to interpret the relevant provisions of BIPA in a more expansive fashion, strict compliance with Illinois's biometric statutory is becoming even more critical to mitigate the already significant liability exposure that exists for non-compliance with the law.

Courts Continue to Interpret BIPA Term "Scan of Face Geometry" in Expansive Fashion

Today, one of the areas of uncertainty in BIPA class action litigation pertains to the precise definition of "scan of face geometry." *See* 740 ILCS 14/15. To date, no court has supplied a definitive definition of the term or otherwise fully analyzed the scope of activities that constitute engaging in scans of face geometry. With that said, courts to date have favored a liberal interpretation of the term. Recently, the US District Court for the Western District of Washington continued that trend in *Wise v. Ring LLC*, No. 20 CV 1298, 2022 U.S. Dist. LEXIS 13899, at *4 (W.D. Wash. Aug. 8, 2022). In that case, the court rejected the argument that video data collected from doorbell cameras (purportedly used to create face templates) of individual bystanders with no contractual relationship to the defendant did not constitute biometric identifiers or biometric information because a mere scan of face geometry – absent identifying information such as a name tying that geometry to a person – did not implicate the risks the Illinois legislature sought to mitigate in enacting BIPA.

Takeaways: As indicated above, the recent plaintiff-friendly interpretations of BIPA should prompt companies that use biometric data in their operations to refocus on their compliance efforts in order to mitigate litigation risk.

Setbacks for Higher Education Defendants in Procuring Dismissals from BIPA Class Actions Under Section 25(c) Financial Institution Exemption

In early 2022, universities and other higher education had some success in obtaining dismissals from BIPA class actions – including the defendants in *Duerr v. Bradley Univ.*, No. 21 CV 1096, 2022 U.S. Dist. LEXIS 86640 (C.D. Ill. Mar. 10, 2022), and *Doe v. Northwestern Univ.*, No. 21 CV 1579, 2022 U.S. Dist. LEXIS 85750 (N.D. Ill. Feb. 22, 2022) – through the utilization of Section 25(c)'s "financial institution" exemption. That exemption provides that BIPA does not "apply in any manner to a financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999 [("GLBA")] and the rules promulgated thereunder[.]" 740 ILCS 14/25(c). More recent decisions, however, have not been as favorable. In both *Harvey v. Resurrection Univ.*, No. 21 CV 3203, 2022 U.S. Dist. LEXIS 154550 (N.D. Ill. Aug. 29, 2022), and *Fee v. Ill. Inst. of Tech.*, No. 21 CV 2512, 2022 U.S. Dist. LEXIS 125581 (N.D. Ill. July 15, 2022), courts rejected attempts to procure dismissals through the assertion of the financial instruction exemption, reasoning that it was inappropriate to make a definitive determination as to whether the defendant universities qualified for the exemption at the motion to dismiss stage.

Takeaways: One of the primary factors leading to the dismissal orders in *Duerr* and *Doe* was the evidence incorporated by reference and of materials from the public record put forth by the defendants in support of their Rule 12(b)(6) motions which established the applicability of the financial institution exemption to those specific defendants who had been targeted for purported BIPA violations. As such, defendants that seek dismissal from BIPA litigation pursuant to their status as a financial institution under the Section 25(c) exemption should ensure that their motions are properly supported, when possible, to allow the court to conclude that BIPA's financial institution exemption applies specifically to the particular activities engaged in by the defendant.

Additional Reading: For more information on how BIPA defendants can maximize their likelihood of obtaining dismissals from class actions utilizing the financial institution exemption as a complete defense to liability, read our team member David Oberly's *Law360* analysis here: A Robust Tool for Defending Against Illinois Biometric Suits.

Employers Continue to Be Sued for BIPA Fingerprint Timekeeping Violations

Following the Illinois Supreme Court's seminal BIPA ruling in *Rosenbach v. Six Flags Ent. Corp.* 2019 IL 123186 (Ill. 2019) in January 2019 – which held that plaintiffs are not required to allege actual injury to pursue claims for purported violations of the law – courts and companies that utilize biometric data in their operations witnessed a drastic spike in the volume of BIPA class action filings, the vast majority of which were asserted in connection with the use of fingerprint time and attendance systems. Now, almost three years later, a high number of employers that use biometric timeclocks continue to be sued for allegedly running afoul of Illinois's biometric privacy statute. Over the course of the last three months, fingerprint timeclock cases were again the most common type of BIPA claim filed in state and federal courts. Of note, the plaintiff's class action bar has continued to focus on this area.

Takeaways: To date, fingerprint time and attendance systems have served as the basis for the largest number of BIPA class action filings. By now, all companies that use biometric timeclocks should seek to have a comprehensive biometric privacy compliance program in place that satisfies BIPA. This includes a publicly available written policy with a retention schedule and data destruction procedures, as well as a mechanism for obtaining written consent before collecting biometric data. If not, they should consult with counsel to bridge any compliance gaps immediately in order to mitigate litigation risk.

Class Action Litigation Developments

First BIPA Class Action Jury Trial

Plaintiff Prevails in First BIPA Class Action Tried Before a Jury to Verdict

On October 12, 2022, the world of biometric privacy litigation experienced a development noteworthy enough to put it on equal footing with *Rosenbach v. Six Flags Ent. Corp.*, 2019 IL 123186, 129 N.E.3d 1197 (Ill. 2019) – which held actual injury is not required to pursue BIPA claims – with a jury finding in favor of a class of Illinois truck drivers in the first BIPA class action to be tried to verdict. In that case, *Rogers v. BNSF Ry.* Co., Richard Rogers alleged that his former employer, BNSF Railway Co., violated BIPA when it collected and stored his and other truck drivers' biometric data without obtaining their consent or informing them of the company's data retention policies. Importantly, however, BNSF itself was not involved in any activities associated with the collection or use of biometric data. Instead, the company contracted with a third-party vendor, Remprex, to operate the equipment that collected Rogers' fingerprints, which purportedly failed to follow the requirements of Illinois's biometric privacy statute. After closing arguments, the jury needed less than an hour to return its verdict in favor of the class of truck drivers. The jury only decided on the issue of liability and was not tasked with calculating damages, which will be assessed by the court at a later date. With that said, using back-of-the-envelope calculations – and assuming that the court applies BIPA's lower $1,000 negligent violation statutory damages amount and awards damages only for the initial finger scan of each class member that ran afoul of the law (as opposed to every scan under a continuing violation theory), damages still amounts to a staggering $44 million.

Takeaways: The potential implications of *Rogers* cannot be overstated. For starters, the fact that a jury needed under an hour to reach its verdict indicates that it was not even a close call in the jurors' eyes as to whether the conduct at issue violated BIPA. In addition, the fact that the jury found against the defendant – despite the fact that the railroad did not itself actively collect, use, or possess any biometric data – provides further support for the critical but unsettled issue of vicarious liability in BIPA class action disputes. Ultimately, the likely impact of the *Rogers* verdict will be an immediate uptick in the volume of BIPA class action filings moving forward. At the same time, the ruling will also almost certainly be used by the plaintiff's attorneys during settlement negotiations to drive up the already-inflated value of BIPA claims. Beyond *Rogers* – the Illinois Supreme Court will soon issue its much-anticipated opinion in *Cothron v. White Castle Sys.*, No. 128004 (Ill Sup. Ct.), which will definitively resolve the currently unsettled issue of claim accrual in BIPA litigation. Depending on how the court answers the question of whether every discrete failure to comply with BIPA's requirements amounts to a separate, independent violation of the statute, the scope of liability exposure and damages underlying BIPA class actions may further increase. Combined, companies that have put off evaluating their biometric data collection and processing practices should do so with the assistance of counsel.

Additional Reading: You can read more about the Rogers verdict and its implications in this *Consumer Privacy World* blog post authored by our team members Kristin Bryan and David Oberly here: Breaking: Plaintiff Prevails in First BIPA Class Action Jury Trial.

Additional Reading: For additional insight on the *Rogers* verdict, you can read this *Legaltech News* article authored by our team member David Oberly here: Analyzing the Impact of the First BIPA Jury Trial on the Biometric Privacy Legal Landscape.

Noteworthy Opinions and Settlements

Snap $35 Million Face Lenses and Filters BIPA Settlement

In August, Snap, the parent company of photo-sharing platform Snapchat, reached a $35 million settlement to resolve ongoing litigation which alleged that the company improperly collected biometric data in violation of BIPA through its Lenses feature (which allows users to add special effects to their Snapchat images) and its Filters feature (which allows users to overlay images onto a pre-existing image framework). Of note, the plaintiffs alleged that to accomplish these effects, Snapchat used smartphone cameras to plot the contours of users' faces and create a digital reference map that connected facial landmarks via 93 points of the user's unique facial characteristics, after which time the app was able to manipulate the spaces between the reference points to change the appearance of the image. Following Snap's successful efforts to compel individual arbitration of the plaintiffs' claims both at the district court level and on appeal, the parties reached a settlement of the litigation prior to scheduled arbitration hearings to avoid the risks, uncertainties, and costs of protracted litigation. The case is *Boone v. Snap Inc.*, No. 2022 LA 708 (Ill. Cir. Ct. DuPage Cnty.).

Takeaways: The Snap settlement illustrates that high settlement awards are becoming the norm, and not the exception, in BIPA class actions. In addition, the Snap settlement is also illustrative of the fact that even where companies do not engage in traditional facial recognition, *i.e.*, activities that involve the identification or verification of individual identities, substantial litigation risk nonetheless exists under BIPA.

TikTok Settlement Receives Final Court Approval

Also in August, an Illinois federal district court granted final approval to the $92 million settlement reached to resolve multidistrict litigation pertaining to alleged BIPA violations involving another popular social media platform, TikTok. In addition to the monetary component of the settlement, the terms agreed to by TikTok also encompass broad injunctive relief, including commitments by TikTok to place limitations on the storage and transmission of data outside the US, deletion of certain user-generated content, implementation of an annual privacy employee/contractor training program, and a three-year privacy auditing period.

Takeaways: The TikTok ligation demonstrates that in addition to sizeable monetary penalties, companies that are found to have violated BIPA may also be required to make modifications to their compliance programs as well in order to resolve biometric privacy class action disputes. As such, companies are well advised to take mitigation now to mitigate BIPA class action risk.

Additional Reading: You can read more about the TikTok settlement and its implications in this *Consumer Privacy World* blog post authored by our team member Kristin Bryan here: TikTok Settlement Receives Final Court Approval.

Rogers v. BNSF Ry. Co., No. 19 CV 3083, 2022 U.S. Dist. LEXIS 173322 (N.D. Ill. Sept. 26, 2022)

On September 26, 2022, the US District Court for the Northern District of Illinois issued one of the first decisions to date on a motion *in limine* filed in BIPA class action litigation in *Rogers*. The *Rogers* court held that vicarious liability may be imposed against a private entity for the purported violations of BIPA committed by a third-party agent.

Takeaways: Companies are well-advised to take note of the court's ruling on the issue of vicarious liability, as this currently unsettled issue has significant implications as it relates to the scope of BIPA liability exposure for entities that utilize third parties to assist in operating their biometrics systems. With the *Rogers* ruling, vicarious liability will remain at least a potentially viable theory of liability in BIPA disputes for the foreseeable future.

Additional Reading: You can read more about the Rogers court's decision on the issue of vicarious liability in this *Legaltech News* article authored by our team member David Oberly here: Takeaways From Recent BIPA Vicarious Liability Decision.

Svoboda v. Frames for Am., Inc., No. 21 CV 5509, 2022 U.S. Dist. LEXIS 162077 (N.D. Ill. Sept. 8, 2022)

As indicated above, online retailers that utilize VTO tools have faced a barrage of class action litigation alleging that their technology runs afoul of BIPA. During this time, a powerful defense has emerged for the targets of VTO suits and online eyewear retailers, in particular – BIPA's health care exemption. Relying on this exemption, in early September, Frames for America, Inc. defeated a class action lawsuit alleging it improperly collected shoppers' face geometry data through its VTO tool in violation of Illinois's biometric privacy statute.

Takeaways: The *Svoboda* opinion demonstrates the power of BIPA's health care exemption, which can serve as a valuable tool for eyewear brands in the defense of BIPA claims to definitively defeat bet-the-company class action lawsuits. At the same time, *Svoboda* also demonstrates the broad scope of the health care exemption and the ability to procure outright dismissals in a wide range of BIPA suits – even those outside the VTO context – through the assertion of this defense, where the facts underlying the litigation involve prescription or non-prescription eyewear.

Additional Reading: You can read more about the *Svoboda* opinion and its implications in this *Legaltech News* article authored by our team member David Oberly here: Dismissal of VTO Class Action Illustrates Power of Health Care Exemption as BIPA Defense.

Wilk v. Brainshark, Inc., No. 21 CV 4794, 2022 U.S. Dist. LEXIS 174271 (N.D. Ill. Sept. 27, 2022)

Today's facial recognition systems have advanced tremendously through the integration of AI tools. These improvements in technology, however, also come with increased liability risks. In particular, AI-powered technology involving the collection and use of biometric data has evolved into an increasingly-common target for BIPA class action lawsuits. Such was the case for Brainshark, Inc., which – with the aid of AI – applies facial-mapping technology to sales professionals' videos for purposes of analyzing individuals' emotions and other performance indicators. In *Brainshark*, a former employee of a Brainshark client sued the company in connection with a video she uploaded to Brainshark at her employer's request. In late September, a federal Illinois court rejected Brainshark's challenge to the plaintiff's complaint, denying the company's motion to dismiss in its entirety. Of note, the court rejected Brainshark's argument that the complaint failed to allege a Section 15(b) violation relating to the collection of biometric data because it only collected videos but not biometric information. In so doing, the court relied heavily on Brainshark's own marketing resources as support for the conclusion that the technology at issue engaged in the scanning of videos for facial features. In addition, the court also referenced the fact that multiple prior decisions had held that what Brainshark allegedly collected and captured by scanning videos qualified as collecting and capturing biometric identifiers.

Takeaways: *Brainshark* serves as a cautionary tale and a reminder of the increasing risks associated with BIPA violations faced by companies that offer AI-powered video analysis or enhancement tools. At the same time, the Brainshark decision also demonstrates that companies should exercise caution when making promotional statements and similar disclosures in their marketing materials to ensure they are not used against them as support for claims asserted in BIPA class litigation.

Trio v. Turing Video, Inc., No. 21 CV 4409, 2022 U.S. Dist. LEXIS 173465 (N.D. Ill. Sept. 26, 2022)

At the onset of the Covid-19 pandemic, many companies turned to devices that incorporated facial recognition technology to enhance workplace safety and minimize the health risks associated with the virus. In so doing, however, the use of this cutting-edge technology also implicates a growing patchwork of biometric privacy laws that can leave employers exposed to litigation risk. Turing Video Inc., which produces and sells a kiosk that allows customers to screen their employees for Covid-19, recently sought dismissal from a BIPA class action alleging that its technology violated Illinois's biometrics statute but was unsuccessful. In that case, a cake decorator, who was required to use Turing's technology as part of her employer's Covid-19 screening process, alleged that the company failed to obtain her informed written consent prior to completing facial scans which collected her facial geometry data and that the company also disclosed her facial data without first obtaining her consent. The court rejected several arguments asserted by Turing in support of dismissal, including the company's contention that the suit was barred by Illinois's extraterritoriality doctrine, finding that the complaint sufficiently alleged the relevant conduct giving rise to the plaintiff's BIPA claims occurred primarily and substantially in Illinois. In addition, the court also held that the plaintiff's allegations that the Turing technology utilized an "artificial intelligence algorithm" to detect individuals' foreheads and take their temperatures, and that the technology used "facial recognition software" to detect whether users were wearing face masks, was sufficient to state plausible claims alleging the "collection" and "possession" of her biometric data, thus defeating the company's contention that the lawsuit warranted dismissal under Rule 12(b)(6) for failure to state a claim.

Takeaways: The *Turing* decision is another example illustrating the wide swath of liability exposure faced by companies that utilize any type of technology that involves detection or analysis of the face.

Additional Reading: You can read more about the legal risks and related implications employers face when implementing facial recognition-powered solutions in this Cincinnati Bar Association *CBA Report Magazine* article authored by our team member David Oberly here: Beware of Biometric Privacy Implications When Using Facial Recognition Technology in the Fight Against Covid-19.

Boyd v. Lazer Spot, Inc., No. 19 CV 8173, 2022 U.S. Dist. LEXIS 131241 (N.D. Ill. July 20, 2022)

In *Boyd v. Lazer Spot, Inc.*, an Illinois federal court rejected the Contribution Act as a defense in BIPA class action litigation. The Contribution Act allows for a defendant to recover contribution from another defendant whose conduct caused the same injury to the plaintiff. In *Boyd*, the court found the Contribution Act to be inapplicable in the context of BIPA because the law holds each entity liable for its own violations. In this respect, according to the court, a plaintiff does not incur one indivisible injury (*e.g.*, a broken leg or lost cargo) caused by multiple defendants but many individual injuries at the hands of many individual defendants who have violated BIPA. Importantly, the court concluded that "each entity is liable for its own violations, 'even if such violations occurred simultaneously or through use of the same equipment" as the violations of another entity.'" As such, the court denied Lazer Spot's request to assert a counterclaim under the Contribution Act. In addition, the court also rejected Lazer Spot's attempted assertion of an affirmative defense relating to the settlement agreement entered into by its vendor, which released all claims against the vendor and its principals – including Lazer Spot. In so doing, the court reasoned that a plaintiff may still recover against a defendant (such as Lazer Spot), even where a settlement agreement has resolved all claims against another defendant (such as Lazer Spot's vendor) that occurred in connection with the same conduct. The court further noted that recovery was permissible against Lazer Spot, despite the existence of the settlement agreement, because the plaintiff's allegations were based on the company's own violations of BIPA, not on whatever its vendor may have done as the company's purported agent.

Takeaways: The *Lazer Spot* opinion appears to limit the ability to assert to reduce a defendant's liability exposure in BIPA class action litigation through the assertion of set-off counterclaims, including those asserted under Illinois's Contribution Act. In addition, the opinion also provides support for the theory that both a vendor and its client can also be held responsible independently for the same alleged BIPA violations – a common scenario that frequently arises in BIPA disputes.

Karling v. Samsara Inc., No. 22 CV 295, 2022 U.S. Dist. LEXIS 121318 (N.D. Ill. July 11, 2022)

In July 2022, a trucking employee sued Samsara, Inc., which supplied facial recognition software cameras and sensors to the trucker's fleet operator employer, for purported violations of BIPA. The employee alleged that Samsara's camera and software collected his and other class members' biometric data without their informed consent and that the company – through its contracts with transportation industry customers – profited from this use. The plaintiff also alleged that Samsara disseminated the biometric data it collected to third parties, including his employer. Samsara filed a Rule 12(b)(6) motion challenging the sufficiency of the trucker's complaint, which was denied. Of note, the *Samsara* court rejected the defendant's argument that the plaintiff's Section 15(a) privacy policy and retention schedule claim should be dismissed because it did, in fact, maintain a publicly-available data retention and deletion policy. In so doing, the court reasoned that the language contained in Samsara's disclosure that the company "keeps facial recognition information for a customer no longer than necessary to provide its Camera ID service to that customer" failed to satisfy the requirements of Section 15(a) because it lacked specific language regarding the company's destruction guidelines.

Takeaways: The *Samsara* court's analysis of the sufficiency of the defendant's privacy policy and data retention/destruction schedule language provides two key takeaways. First, companies should provide disclosures on two discrete matters with respect to the issue of data retention/destruction to satisfy this component of Section 15(a): (1) a retention schedule; and (2) guidelines for permanently destroying biometric identifiers and information. Second, companies should take care to ensure they provide a sufficient level of detail regarding their disclosures as it relates to the permanent destruction of biometric data. In this regard, boilerplate language, such as retaining data "no longer than necessary" – which the *Samsara* court found insufficient to satisfy Section 15(a) – should be avoided.

Additional Reading: For a more in-depth discussion of the Samsara decision and its implications, you can read this *Consumer Privacy World* blog post authored by our team member Kristin Bryan here: Federal Court Refuses to Dismiss Biometric Claims Brought by Trucker Against Facial Recognition Company.

Cases to Keep on Your Radar

Marschke v. YouTube, LLC, No. 3:22-cv-2022 (S.D. Ill.)

Large technology companies continue to be primary targets of BIPA class actions, especially as it relates to features that – at least, again, according to the plaintiff's counsel – appear to engage in scans of face geometry. In *Marschke v. YouTube, LLC*, YouTube was hit with a BIPA class action in connection with its Face Blur and thumbnail tools offered to YouTube content creators. According to the complaint, the Face Blur tool allegedly allows content creators to select specific faces appearing in their videos, which are then blurred to make them unrecognizable when viewed by others on YouTube's platform. The thumbnail feature purportedly operates by automatically scanning uploaded videos to identify still frames within a video containing faces and then making those images available to content creators, who are able to select the thumbnail of their choice to be displayed as the video's "preview" image. The *Marschke* plaintiff alleges that both features operate by capturing and storing face geometry scans.

Takeaways: The *Marschke* class action provides an example of the increased risks companies now face when offering product features that could implicate facial recognition and scans of face geometry – which the plaintiff's attorneys have become well-versed in using to allege purported BIPA violations.

Skinner v. ID.me Inc., No. 22 CH 7688 (Ill. Cir. Ct. Cook Cnty.)

Identity verification companies have also become an increasingly popular target for BIPA class actions as well. In *Skinner v. ID.me Inc.*, a former Chicago hospital employee filed suit against her prior employer's identity verification vendor, ID.me, for purported violations of BIPA's data retention and destruction requirements. According to the complaint, the plaintiff's former employer required her to create an account with ID.me and upload a photograph of her face for identity verification purposes. However, when she did so, ID.me's data retention policy provided that the vendor would maintain users' biometric identifiers and information for up to seven and a half years after an individual canceled their ID.me account – over four years longer than BIPA's mandatory three-year data retention limitation.

Takeaways: The *Skinner* class action is only one of a number of BIPA complaints filed against identity verification companies in the last three months. If they have not already done so, companies that perform identity verification services should consult with counsel to ensure their operations are fully compliant with BIPA and related biometric privacy laws to mitigate litigation risk.

Guy-Powell v. Applebee's Restaurants LLC, No. 22 CH 8365 (Ill. Cir. Ct. Cook Cnty.)

In late August, a number of restaurant chains were sued for purported violations of BIPA in connection with their use of AVO systems that utilize AI to facilitate customer phone orders, answer customer questions, give directions, and respond to other customer and restaurant needs. According to the complaint, the restaurants' AVO systems capture and store voiceprint data without first providing notice and obtaining consent in violation of BIPA. In addition, the complaint alleges that collected voiceprints are also used for internal purposes to train and improve the restaurant's voice technology, but that this use is not disclosed to consumers.

Takeaways: While facial recognition and fingerprints remain the top two biometric modalities targeted for BIPA class action complaints, an increasing number of suits targeting voice biometrics have been filed over the course of 2022. Unlike facial recognition and fingerprint systems, voice biometrics solutions often involve more complexity in terms of satisfying BIPA's Section 15(b) notice and consent requirements. Importantly, however, as established in *Neals v. PAR Tech Corp.*, 419 F. Supp. 3d 1088, 1092 (N.D. Ill. 2019), arguments that a company has "no feasible means to obtain consent" are insufficient to defeat claims alleging a violation of BIPA's prior written consent requirement. Thus, companies utilizing voiceprints in their operations should ensure that they provide notice and obtain consent from all individuals prior to the time they collect any voice biometric data.

Kukovec v. L'Oreal USA Inc., No. 1:22-cv-3829 (N.D. Ill.)

In *Kukovec v. L'Oreal*, an Illinois resident filed suit against the cosmetics retailer for purported BIPA violations arising out of her use of the company's VTO tool to test how a lipstick would look if applied to her face. Based on her one-time use of the VTO tool, the plaintiff asserts two counts under BIPA – one, under Section 15(b), for the company's alleged failure to provide written disclosures or obtain a written release prior to collecting her biometrics; and another, under Section 15(a), for allegedly failing to develop a publicly-available privacy policy as required by the statute. Recently, the retailer moved for dismissal of the class action on several grounds, including failure to state a claim because she expressly consented to a BIPA-compliant privacy policy, as the VTO tool at issue is only accessible if consumers, such as the plaintiff, first consent to the privacy policy that contains all BIPA-mandated disclosures.

Takeaways: As *Kulovec* demonstrates, BIPA suits targeting online retailers and their use of VTO tools continue to be filed at a high frequency, with no signs of slowing down for the foreseeable future. Of note, the impending decision in *Kukovec on L'Oreal's* motion to dismiss will likely provide insight as to the level of detail that is required to be included in biometrics-specific privacy policies to satisfy the requirements of this specific component of the law. Make sure to check *Consumer Privacy World* regularly, as we will be there to keep you in the loop.

Kashkeesh v. Microsoft Corp., No. 1:21-cv-3299 (N.D. Ill.)

In *Kashkeesh v. Microsoft Corp.*, two Uber drivers whose identities were verified through Microsoft's Real-Time ID Check – which requires drivers using the app to share a selfie to ensure they match the approved individual Uber has on file as the account holder – sued the company for alleged violations of BIPA's privacy policy/data destruction, informed consent, sales/profiting ban, and disclosure requirements. At the end of June, a federal court remanded the plaintiffs' privacy policy data/destruction and sales/profiting ban claims back to state court as a result of the absence of standing on the part of the individuals to maintain these components of their action in federal court. More recently, at the end of August, Microsoft moved for the dismissal of the remaining federal court claims on personal jurisdiction grounds, arguing that the plaintiffs could not maintain their suit in Illinois simply because one of its customers made the unilateral decision to use the identity verification application within the borders of the state.

Takeaways: *Kashkeesh* is illustrative of the trend that has continued throughout 2022 of BIPA suits targeting companies that offer biometric technology solutions to corporate clients, but which maintain no direct relationship with consumer end users. Importantly, vendors and service providers should remain cognizant of the fact that despite the lack of any direct relationship, whether compliance with BIPA is required by entities that do not directly collect data from employees, customers, or similar classes of individuals remains an unsettled issue. As such, to mitigate potential liability exposure, these third parties should satisfy Illinois's biometric statute whenever feasible. In addition, readers should also keep their eyes on this case as we head toward the end of 2022, as the litigation may offer companies and their counsel guidance on this critical yet unresolved issue.

Legislative/Regulatory Developments

White House Issues AI Bill of Rights Blueprint

The White House Office of Science and Technology Policy ("OSTP") recently issued its Blueprint for an AI Bill of Rights, which seeks to help guide the design, development, and deployment of AI and automated systems so that they protect the rights of the American public. The AI Bill of Rights is designed to apply broadly to all automated systems that have the "potential" to significantly impact individuals or communities concerning matters that include privacy, civil rights, equal opportunities for healthcare, education, employment, and access to resources and services. Of note, the AI Bill of Rights set forth five categories of core protections designed to protect the rights of Americans in the age of AI: (1) safe and effective systems; (2) algorithmic discrimination protections; (3) data privacy; (4) notice and explanation; and (5) human alternatives, consideration, and fallback. This effort is intended to further the ongoing discussion regarding privacy among federal government stakeholders and the public and to support the development of policies and practices that protect civil rights and promote democratic values in the building, deployment, and governance of automated systems, but is non-binding and does not constitute US government policy.

Takeaways: The White House's AI Bill of Rights Blueprint is the latest attempt by the executive branch to aid in the development of a governance framework for AI tools. In addition to these efforts by the executive branch, Congress is also currently focusing on implementing greater regulation over the use of AI tools with its proposed Artificial Intelligence Act ("AIA"), which was re-introduced in March of this year. If enacted, the AIA would provide the FTC with broad powers to regulate the commercial use of AI tools while also imposing a nationwide mandate that would require companies to complete impact assessments to evaluate companies' tools for accuracy and bias/discrimination and "reasonably address in a timely manner" any identified biases or related issues.

Additional Reading: To learn more about the AI Bill of Rights and its implications, you can read this *Consumer Privacy World* blog post authored by our team members Kristin Bryan, Beth Goldstein, Jeff Turner, and Kyle Fath here: White House Office of Science and Technology Policy Releases AI Bill of Rights.

FTC Issues Advanced Notice of Proposed Rulemaking, Indicates Focus Will Continue on Policing AI and Facial Recognition

As noted above, on August 11, 2022, the FTC issued its Commercial Surveillance ANPR, seeking public comment on whether new trade regulation rules are needed to protect people's privacy and information. The Commercial Surveillance ANPR is broad, seeking comment on 95 questions relating to harms stemming from commercial surveillance and lax data security practices. From a general perspective, the Commercial Surveillance ANPR provides key insight on the specific practices and associated harms viewed by the Commission as most concerning and potentially in need of greater enforcement. Importantly, a significant portion of the Commercial Surveillance ANPR focuses more narrowly on issues relating to AI and automated decision-making and whether the FTC should promulgate new rules to regulate or otherwise limit the use of this type of advanced technology. Specifically, 21 of the 95 questions set forth in the Commercial Surveillance ANPR relate to concerns regarding AI tools. In addition to the questions themselves, the Commercial Surveillance ANPR also provides a fairly detailed discussion regarding the Commission's discrimination and bias concerns as they relate to the use of AI technologies.

Takeaways: Companies that employ AI tools and algorithmic decision-making models should make sure to monitor future developments regarding the FTC's ongoing Section 18 rulemaking efforts so that they can stay ahead of all relevant future AI developments.

New York City Issues Proposed Rules to Clarify Ambiguities in New Automated Employment Decision Tools Ordinance

On September 23, 2022, the New York City Department of Consumer and Worker Protection ("DCWP") published Proposed Rules for implementation of the Big Apple's AI-focused automated employment decision tools ("AEDT") ordinance. The proposed rules resolve some ambiguities and provide clarity as to the compliance obligations imposed on employers that are covered by the ordinance. Of note, the guidance provides significant detail on the completion of bias audits mandated under the ordinance, including requirements that employers calculate the "selection rate" and "impact ratio" relating to their AI tools and the impact they have on individuals based on race, ethnicity, and gender. The DCWP will hold a public hearing on the Proposed Rules on Monday, October 24, 2022.

Takeaways: Employers that operate in New York City or recruit candidates from the Big Apple should ensure they are in strict compliance with the AEDT Ordinance by the start of 2023, which will require employers to conduct bias audits of their AI tools, make several key public disclosures, and have mechanisms in place for providing job candidates and employees with individualized notice (among other things). Because bias audits should be completed by January 1, 2023, covered businesses should begin the audit process immediately if they have not already done so.

CFPB Warns Digital Marketing Providers to Comply with Federal Consumer Finance Protections

On August 10, 2022, the CFPB issued an Interpretive Rule, *Limited Applicability of Consumer Financial Protection Act's "Time or Space" Exception With Respect to Digital Marketing Providers*, which warns that digital marketing providers need to comply with federal consumer finance protections and cautions technology firms that use behavioral targeting in connection with financial products that they will be held liable for violations of the Consumer Financial Protection Act ("CFPA"). The CFPB highlights that financial firms now often rely on the expertise and tools of digital marketing providers that offer sophisticated analytic techniques, aided by machine learning and advanced algorithms, to process large amounts of personal data and deliver highly targeted ads. Depending on how these practices are designed and implemented, these behavioral marketing and advertising activities could cause marketing companies to be classified as "service providers" under the CFPA and thereby subject them to the CFPB's jurisdiction and the Bureau's unfair, deceptive, and abusive acts or practices ("UDAAP") authority.

Takeaways: In its Interpretive Rule, the CFPB indicates its increased concern regarding UDAAPs and related discriminatory actions relating to the selection and placement of advertising in the financial services sector. As the CFPB has recently stepped up its efforts to more closely scrutinize potential discrimination and bias in connection with the use of AI tools and associated algorithms, marketing companies should take time to assess their current operations to mitigate risk.

CFPB Takes Action Against Hello Digit for Lying to Consumers About Its Automated Savings Algorithm

In mid-August, the CFPB entered into a Consent Order with Hello Digit, LLC, a financial-technology ("FinTech") company that offers consumers an automated-savings tool which uses a proprietary algorithm to make automatic transfers from consumers' checking accounts, termed "auto-saves," to an account held in Hello Digit's name. Hello Digit represented that the tool "never transfers more than you can afford," provided a "no overdraft guarantee," and represented that, in the unlikely event of an overdraft, Hello Digit would reimburse consumers. The CFPB found that Hello Digit engaged in deceptive acts and practices because, in reality, the company's automated savings tool routinely caused consumers' checking accounts to overdraft and Hello Digit did not always reimburse consumers for overdraft fees caused by its algorithmic auto-save tool. The Consent Order enjoins Hello Digit from making any misrepresentations related to its auto-save tool and requires the company to provide at least $68,145 in redress to consumers who were denied reimbursement requests for overdraft fees caused by the AI tool. In addition, Hello Digit must also pay a $2.7 million penalty.

Takeaways: The Consent Order issued against Hello Digit indicates that moving forward, the CFPB will likely be active in investigating and pursuing instances where the use of algorithms results in improper adverse consumer outcomes – even those that fall outside of the scope of the fair lending context. As such, all FinTech companies should review their algorithms and associated models regularly to ensure they do not run the risk of violating applicable consumer protection laws or otherwise opening the door to a CFPB investigation.

CFPB Creates New Office of Competition and Innovation, Continuing to Intensify Its Focus on FinTech, AI, and Machine Learning

The CFPB also recently revamped its approach to innovation with the creation of the agency's new Office of Competition and Innovation, which replaces the CFPB's prior Office of Innovation and Operation Catalyst. In issuing the announcement, CFPB Director Rohit Chopra noted that "[c]ompetition is one of the best forms of motivation. It can help companies innovate and make their products better and their customers happier. [The CFPB] will be looking at ways to clear obstacles and pave the path to help people have more options and more easily make choices that are best for their needs." In addition, the agency also scrapped its No-Action Letter and Compliance Assistance Sandbox programs, which the CFPB found to be ineffective and had led to some participating firms making public statements that the CFPB had conferred benefits upon them that the agency, in fact, had not afforded them.

Takeaways: Over the course of the last two years, the CFPB has issued a range of policy guidance and legal interpretations on AI-related issues relevant to financial institutions, illustrating the sustained focus that the CFPB has placed on ensuring the proper use of AI.

In turn, it is likely that all companies that operate in the market for consumer financial services will see enhanced regulatory scrutiny by the agency regarding the use of AI, as well as an increase in the number of enforcement actions pursued against those organizations that the agency believes are violating consumer financial laws in connection with the use of AI and algorithmic decision-making. As such, entities subject to the CFPB's jurisdiction should familiarize themselves with applicable laws and regulations that implicate the use of AI, as well as the CFPB's recent supervisory guidance and related announcements pertaining to algorithmic decision-making.

National Institution of Standards and Technology Releases Second Draft of AI Risk Management Framework and Playbook for AI Best Practices

The National Institution of Standards and Technology ("NIST") recently issued the second draft of its Artificial Intelligence Risk Management Framework ("AI RMF"), as well as its draft companion Playbook to the AI RMF. The AI RMF has been developed to aid companies in better managing risks to individuals, organizations, and society associated with AI and is intended for voluntary use to improve the ability to incorporate trustworthiness considerations into the design, development, use, and evaluation of AI products, services, and systems. The Playbook provides recommended actions Framework users can take to implement the AI RMF by incorporating trustworthiness throughout the AI system life cycle, as well as additional references and documentation guidance for stakeholders.

Takeaways: Companies that use or intend to use AI in their operations should pay close attention to future developments and the release of the final version of the AI RMF and Playbook, as – although the AI RMF does not promulgate binding legal requirements – these materials are nonetheless likely to have a tangible impact on the direction of industry standards in this space.

Upcoming Webinars

Federal Privacy Legislation: Within Reach After a Decade of Debate. If So, What Next?
Lexology, Dec. 7, 2022 | Kristin Bryan, Beth Goldstein & Jeffrey Turner

Recent Webinars, Expert Commentary and Publications

Webinars/Seminars

Biometrics Are Back! (And So Are the Lawsuits), *American Bar Association 16th Annual Section of Labor and Employment Law Conference* | David Oberly

CPW Team Members Kyle Fath and Gicel Tomimbang Discuss Privacy & AI With IBM's Chief Privacy Officer and AI Ethics Board Chair, *IAPP* | Kyle Fath and Gicel Tomimbang

Expert Commentary

Biometric Privacy Perils Grow After BNSF Loses Landmark Verdict, *Bloomberg Law* | David Oberly

As Virtual Try-On Fashion Technology Grows, So Do Legal Risks, *Bloomberg Law* | David Oberly

Consumer Privacy World Blog Posts

Federal Court Dismisses Biometric Privacy Class Action Brought Against University, On Basis It Was Regulated "Financial Institution", *Consumer Privacy World* | Kristin Bryan, David Oberly and Ekaterina Long

Recent BIPA Opinion Illustrates Continued Uncertainty Underlying Core Issues in Biometric Privacy Class Action Litigation, *Consumer Privacy World* | Kristin Bryan and David Oberly

Breaking: Plaintiff Prevails in First BIPA Class Action Jury Trial, *Consumer Privacy World* | Kristin Bryan and David Oberly

White House Office of Science and Technology Policy Releases AI Bill of Rights, *Consumer Privacy World* | Kristin Bryan, Beth Goldstein, Jeff Turner and Kyle Fath

Available Now: CPW's Kristin Bryan, Christina Lamoureux, and Margaret Booz Co-Author Lexis Practice Note on Biometric Privacy and AI Legal Developments, *Consumer Privacy World* | Kristin Bryan, Christina Lamoureux and Margaret Booz

Congratulations to CPW's Kristin Bryan on Being Named a 2022 Cybersecurity & Privacy MVP by Law360!, *Consumer Privacy World* | Kristin Bryan

Our Data Privacy Practice Continues to Expand: Julia B. Jacobson and Shea Leitch Join the Team, *Consumer Privacy World*

CPW's Kyle Fath and Gicel Tomimbang Speak at IAPP Webinar on Privacy and AI, *Consumer Privacy World* Kyle Fath and Gicel Tomimbang

CPW's David Oberly Discusses Practical Tips for Building Comprehensive Biometric Privacy Programs to Manage Legal Risks and Mitigate Liability Exposure in Biometric Update, *Consumer Privacy World* | David Oberly

TikTok BIPA Settlement Receives Final Court Approval, *Consumer Privacy World* | Kristin Bryan

Federal Court Rejects Terms in Franchise Agreement Retaining Data Access Rights As Sufficient to Plead Section 15(b) BIPA Claim, *Consumer Privacy World* | Kristin Bryan and David Oberly

Breaking: The FTC Issues Advanced Notice of Public Rulemaking for Privacy Regulations, *Consumer Privacy World* | Kristin Bryan, Kyle Fath and Marissa Black

CPW's David Oberly Discusses Biometric Privacy Compliance Strategies in Advance of Cothron BIPA Claim Accrual Ruling in Biometric Update, *Consumer Privacy World* | David Oberly

Artificial Intelligence and the Risk of Bias in Recruitment Decisions, *Consumer Privacy World* | Malcolm Dowden and Lucia Harnett

CPW's David Oberly to Participate in Panel Presentation on Tsunami of BIPA Class Action Suits & Impact on Employer Biometrics Practices at ABA Section of Labor & Employment Annual Conference, *Consumer Privacy World* | David Oberly

Federal Court Refuses to Dismiss Biometric Claims Brought by Trucker Against Facial Recognition Company, *Consumer Privacy World* | Kristin Bryan

Online Webinar Now Available: Kristin Bryan and Kyle Fath Discuss AI and Biometric Privacy Trends and Developments, *Consumer Privacy World* | Kristin Bryan and Kyle Fath

Published Articles

Financial Institution Exemption Dooms Student's BIPA Class Action Suit, *Biometric Update* | David Oberly

FTC Signals Intent to Increase Regulation Over AI Tools in Recent Report to Congress, *American Bar Association Cybersecurity & Data Privacy Committee Newsletter* Kristin Bryan, Kyle Fath and David Oberly

Takeaways From EEOC Guidance on Use of AI in Hiring & Employment Decisions, *American Bar Association Cybersecurity & Data Privacy Committee Newsletter* David Oberly

Analyzing the Impact of the First BIPA Jury Trial on the Biometric Privacy Legal Landscape, *Legaltech News*, David Oberly

Takeaways From Recent BIPA Vicarious Liability Decision, *Legaltech News* | David Oberly

Dismissal of Virtual Try-On Class Action Illustrates Power of Health Care Exemption as BIPA Defense, *Legaltech News* David Oberly

Beyond BIPA: Mitigating Biometric Data Legal Risks Under Texas and Washington Biometrics Laws, *Biometric Update* David Oberly

Compliance Tips in Advance of Cothron Illinois Supreme Court BIPA Claim Accrual Ruling, *Biometric Update* David Oberly

Kristin Bryan
Partner, New York

Kyle Fath
Partner, New York and Los Angeles

Julia Jacobson
Partner, New York

David Oberly
Senior Associate, Cincinnati

Brittany Silverman
Associate, Columbus

Alexandra (Shasha) Kiosse
Associate, New York