Biometric Privacy and Artificial Intelligence Legal Developments

Go to: Legal Issues and Litigation Trends concerning Biometric Data | AI Developments
Maintained

by Kristin Bryan, Christina Lamoureux, and Margaret Booz, Squire Patton Boggs

This practice note discusses emerging legal issues concerning the collection, use, and disclosure of biometric data and artificial intelligence (AI). Specifically, this note addresses the legal regimes often implicated in lawsuit trends that are likely a harbinger of future litigation, recent developments concerning Article III standing, damages, and class certification/settlement, among other considerations. As always, litigating complex data privacy cases requires retention of counsel experienced in this continually evolving and complex area of the law.

For more information on litigation in data security and privacy, see Privacy, Cybersecurity, and Data Breach Litigation: Key Laws and Considerations. For more on biometrics, see Biometric Privacy: Mitigating Legal Risks When Using Biometric Technologies, Biometrics Workplace Compliance and Best Practices for Employers, Biometrics and Data Privacy Podcast, Biometric Privacy Compliance Checklist, and Biometric Privacy State Law Survey.

For more on artificial intelligence, see Big Data Analytics Privacy Law Considerations. Also see Artificial Intelligence and Automation in E-Commerce and Artificial Intelligence Key Legal Issues in Practical Guidance's Commercial Transactions practice area, and Artificial Intelligence and Robots in the Workplace: Best Practices in Practical Guidance's Labor & Employment area.

For related news, see How Ill. High Court Ruling May Further Evolve BIPA Landscape, Cybersecurity & Privacy Cases To Watch In 2022, Google becomes latest tech giant stung by Illinois privacy law, agrees to $100 million settlement, No Actual Injury Needed for Suit Under Biometric Privacy Law, Illinois High Court Rules, The New Class Action Frontier Under Illinois Privacy Law, BIPA Bares Its Teeth In Facebook Biometric Privacy Deal, and Comment: US Federal Trade Commission warns AI abuses will be regulatory focus.

Legal Issues and Litigation Trends concerning Biometric Data

The most familiar biometric privacy legislation to practitioners is the Illinois Biometric Privacy Act, which has spurred extensive and high stakes litigation in recent years. It has also brought up many common and currently unsettled legal issues, emerging trends, class action litigation considerations, and pending legislation in other states.

The Illinois Biometric Information Privacy Act

Illinois' Biometric Information Privacy Act (BIPA), the first major biometric privacy law in the United States, was passed in 2008 to protect the privacy of biometric information of Illinois residents. "Biometric information" includes any information based on biometric identifiers that identifies a specific person—regardless of how it is captured, converted, stored, or shared. 740 Ill. Comp. Stat. Ann. 14/10. "Biometric identifiers" include" a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry." 740 Ill. Comp. Stat. Ann. 14/10. You should be familiar with each of the three distinct subsections of BIPA:

- **General notice.** Section 15(a) requires a company to publicly post a general notice about the company's biometric data retention periods. 740 Ill. Comp. Stat. 14/15(a).
- **Specific notice and consent.** Section 15(b) requires a company to provide specific notice and obtain consent from the particular person whose biometric information is collected. 740 Ill. Comp. Stat. 14/15(b).
- **Ban on sale or trade.** Section 15(c) bans the sale or trade of personal biometric information for profit. 740 Ill. Comp. Stat. 14/15(c).

Notably, BIPA provides a private right of action for anyone aggrieved by a violation and allows for liquidated statutory damages. 740 Ill. Comp. Stat. 14/20. This has led to BIPA becoming one of the most frequently litigated privacy statutes in the nation. Plaintiffs bringing suit under BIPA may seek actual damages or liquidated damages of either $1,000 per violation for negligent violations or $5,000 per violation for intentional or reckless violations.

Common Issues Raised in BIPA Litigations

Although BIPA went into effect in 2008, unresolved issues continue to surface in BIPA litigations. In 2022, the Illinois Supreme Court may clarify some of the most significant and common questions, including:

- When BIPA claims accrue (and how to calculate damages)
- The statute of limitations applicable to BIPA claims –and–
- Whether plaintiffs who bring BIPA claims in Illinois state court have standing in federal court

As a privacy attorney, you should be aware of how these pending appeals could impact your practice with respect to BIPA.

Claim Accrual and Damages

The most significant currently unsettled issue in BIPA litigations is whether a BIPA claim accrues when biometric data is collected in the first instance, or whether a defendant can commit reoccurring violations of the statute—such as whenever an employee clocks in or clocks out—with liquidated statutory damages available with each independent collection.

This issue is currently pending before the Illinois Supreme Court in Cothron v. White Castle Sys., 20 F.4th 1156 (7th Cir. 2021). The plaintiff brought suit against her former employer seeking damages for each independent collection of her biometric data when she scanned her fingerprint to access her work computer. In December 2021, the Seventh Circuit Court of Appeals certified to the Illinois Supreme Court the question: "Do section 15(b) and 15(d) claims accrue each time a private entity scans a person's biometric identifier and each time a private entity transmits such a scan to a third party, respectively, or only upon the first scan and first transmission?" Cothron, 20 F.4th at 1167. The Seventh Circuit observed: "Whether a claim accrues only once or repeatedly is an important and recurring question of Illinois law implicating state accrual principles as applied to this novel state statute. It requires authoritative guidance that only the state's highest court can provide." Cothron, 20 F.4th at 1159.

This case is worth watching, as its resolution will have a significant impact on future BIPA litigations, particularly putative class actions. The potential to recover for each individual collection (rather than only the first collection) would exponentially increase damages calculations. The Illinois Supreme Court's ruling may also impact other state biometric and privacy laws that incorporate consent requirements and liquidated damages through a private right of action similar to BIPA.

Standing

Defendants in BIPA litigations commonly remove BIPA litigations to federal court. In response, BIPA plaintiffs frequently seek to strategically limit their claims in an effort to avoid the imposition of Article III standing and preclude removal.

Article III standing is necessary to maintain suit in federal court and requires that a plaintiff be able to demonstrate (1) a concrete injury in fact; (2) causation, or that the injury was caused by the defendant; and (3) redressability, or that the injury would likely be redressed by the requested relief. Under the Illinois Supreme Court's ruling in *Rosenbach v. Six Flags Ent'mt Corp.*, an alleged statutory violation of BIPA is sufficient to bring a BIPA claim in state court. 129 N.E.3d 1197, 1207 (Ill. 2019). However, the standard is different for litigating BIPA claims in federal court, as the Supreme Court has clarified that Article III standing requires more than just a bare procedural violation. Spokeo v. Robins, 136 S. Ct. 1540, 1549 (2016).

Several key Seventh Circuit decisions have continued to shape the standing inquiry, which differs for each subsection of BIPA. Generally, Section 15(a) claims are highly fact-dependent on the allegations pled in each unique case, while Section 15(b) claims are typically permitted to proceed because the harms implicated are inherently particularized. The decisions include:

- **Bryant v. Compass Grp. USA, Inc., 958 F.3d 617 (7th Cir. 2020).** BIPA plaintiffs had standing to recover damages in federal court for the alleged violations of Section 15(b), but not Section 15(a), because a failure to follow Section 15(b) leads to an invasion of personal rights that is both concrete and particularized.
- **Fox v. Dakkota Integrated Sys., 980 F.3d 1146 (7th Cir. 2020).** Standing for a Section 15(a) claim depended on the particular allegations pled, and the plaintiff had sufficiently alleged facts to satisfy standing stemming from the defendant's Section 15(a) violation resulting in the wrongful retention of her biometric data after her employment ended.
- **Thornley v. Clearview AI, 2021 U.S. App. LEXIS 1006 (7th Cir. Jan. 14, 2021).** The plaintiffs lacked Article III standing when the complaint alleged procedural violations only for a Section 15(a) claim.

In addition to extensive BIPA litigation, other recent legal actions concerning AI and biometrics indicate that mere procedural violations of a privacy statute cannot confer Article III standing. In Elec. Priv. Info. Ctr. v. United States Postal Serv., 2022 U.S. Dist. LEXIS 54568 (D.D.C. Mar. 25, 2022), the Electronic Privacy Information Center (EPIC) filed a lawsuit on behalf of itself and its members, alleging that the U.S. Postal Service failed to comply with the E-Government Act by using facial recognition and social media monitoring to identify potential threat actors without conducting a privacy impact assessment. The court dismissed the claims on the ground that EPIC lacked both organizational standing and individual members' standing to sue.

Statute of Limitations

Although BIPA provides a private right of action, the statute does not clarify the applicable statute of limitations to bring a BIPA claim. The Illinois Code provides for three possible statutes of limitations that could apply to BIPA claims: (1) one year (for publication of matter violating the right to privacy), (2) two years (for personal injury suits), or (3) five years (for civil actions not otherwise specified).

Most recently, a panel for the Illinois Court of Appeals held that the one-year limitation period under 735 Ill. Comp. Stat. Ann. 5/13-201 governs BIPA actions under Section 15(c) and (d) while the five-year period under 735 Ill. Comp. Stat. Ann. 5/13-205 governs BIPA actions under Section 15(a), (b), and (e). In Tims v. Black Horse Carriers, Inc., 184 N.E.3d 466 (Sept. 17, 2021), the court observed that, unlike claims under Section 15(c), "an action under section 15(a), (b), or (e) of the Act is not an action 'for publication of matter violating the right of privacy," because "[a] plaintiff could bring an action under the Act alleging violations of section 15(a), (b), and/or (e) without having to allege or prove that the defendant private entity published or disclosed any biometric data to any person or entity beyond or outside itself." Tims, 184 N.E.3d at 497.

Although the shorter limitations period adopted for BIPA claims under Section 15(c) and 15(d) is a welcome ruling for defendants named in BIPA class actions, this ruling is poised to have a limited impact on pending and future-filed BIPA cases. With the statute's provision for generous liquidated damages, class actions will still potentially bring a significant payoff for determined class counsel, even if classes are defined depending on the claim asserted to include only a one-year period.

Emerging Trends in Biometric Data and BIPA Litigation

In addition to the trends described above, BIPA litigators should take note of several emerging trends in BIPA litigations that are anticipated to continue throughout 2022.

Unlawful Profiting Claims

740 Ill. Comp. Stat. Ann. 14/15(c) prohibits private entities from selling, leasing, trading, or otherwise profiting from a person's or a customer's biometric identifier or biometric information. Section 15(c). An increasing number of BIPA actions involve unlawful profiting claims often based on a defendant's alleged use of biometric data in creating a profit or service, or a defendant's emphasis on biometric data in its advertising, leading to increased profits.

The Western District of Washington has clarified the issue of what constitutes an actionable "profit." In Vance v. Microsoft Corp., 534 F. Supp. 3d 1301 (W.D. Wash. 2021), and in Vance v. Amazon.com Inc., 534 F. Supp. 3d 1314 (W.D. Wash. 2021), the court interpreted Section 15(c) as regulating transactions with two components: (1) access to biometric data is shared or given to another; and (2) in return for that access, the entity receives something of value. Microsoft, 534 F. Supp. 3d at 1307; Amazon, 534 F. Supp. 3d at 1322.

Based on the same analysis, the court found that the plaintiffs had sufficiently stated a claim in the *Amazon* litigation by alleging that a face-matching tool was so incorporated into the defendant's product that by marketing the product, it was commercially disseminating the biometric data. However, the court dismissed the plaintiffs' Section 15(c) claims in the *Microsoft* litigation where the plaintiffs had simply alleged that the defendant used biometric data to improve its own facial recognition products and technologies.

BIPA litigators should anticipate similar claims, as the plaintiffs will likely continue to test the boundaries of when a defendant is profiting from biometric data.

Federal Preemption

A common defense in BIPA actions is that the claims are preempted by federal law. In several notable decisions, courts have sided with the defendants and dismissed the plaintiff's claims on the basis of federal preemption. In Miller v. Southwest Airlines Co., 926 F.3d 898 (7th Cir. 2019), the Seventh Circuit dismissed BIPA claims filed by unionized airline workers as preempted by federal law, finding that the workers were required under the Railway Labor Act to bring BIPA claims before an adjustment board, as the collective bargaining agreement in place was required to be interpreted under federal law. 926 F.3d 898, 903 (see also Crooms v. Sw. Airlines Co., 2020 U.S. Dist. LEXIS 84360 (N.D. Ill. May 12, 2020)).

However, federal preemption is far from a sure thing in BIPA suits, particularly at an early stage in the litigation. For example, in Fleury v. Union Pac. R.R. Co., 2021 U.S. Dist. LEXIS 55766 (N.D. Ill. Mar. 24, 2021), the court denied a motion to dismiss a truck driver's lawsuit primarily on the basis that two federal statutes, the Federal Railroad Safety Act and the Interstate Commerce Commission Termination Act, preempted BIPA. The court found that the defendant's argument was premature based on a dearth of facts in the record.

Virtual Try-On Litigation

BIPA litigation in the past two years has seen a wave of class action suits filed against retailers—including fashion, eyewear, and makeup brands—with virtual try-on (VTO) tools offered to online shoppers. As the name suggests, VTO tools, also known as virtual mirrors, allow shoppers to "try on" products using their camera-equipped devices, such as home computers, tablets, or mobile phones. VTO technology is powered by a combination of AI and augmented reality, as opposed to traditional facial recognition technology used to identify or verify an individual's identity. Despite this, many brands found themselves the targets of BIPA class litigation, with the plaintiffs arguing that their VTO technology performed scans of face geometry, bringing the tools within BIPA's scope.

One such brand was Louis Vuitton, which became the subject of a class action in April of 2022. In Theriot v. Louis Vuitton N.A., Inc., No. 1:22-cv-02944 (S.D.N.Y. April 8, 2022), shoppers alleged BIPA violations with the company's VTO website tool. The complaint alleged that the tool scans users' face geometry to try on its designer eyewear without giving notice or obtaining consent. As VTO facial recognition class actions continue to be a hot trend in BIPA litigation (as discussed in more detail below), retailers and other companies that utilize this "try before you buy" technology should ensure they are strictly complying with the mandates of BIPA to mitigate the significant class action risks associated with these tools.

Suits against Third-Party Vendors

There has been a marked increase in BIPA class actions targeting third-party vendors that offer biometric technology software and solutions, such as identity verification tools and employee time clocks. Of note, these vendors do not maintain any direct relationship with the individuals who claim their biometric data was collected or used in violation of BIPA. Rather the vendors' technology is merely utilized by their clients to facilitate the use of biometric data in commercial operations.

One key case representing this trend is Mahmood v. Berbix, Inc., 2022 U.S. Dist. LEXIS 153010 (N.D. Ill. Aug. 25, 2022). "Selfie" identity verification has become extremely popular due to its speed, accuracy, and fraud reducing benefits. At the same time, companies that develop and supply this technology have become an increasingly common target for BIPA class action suits. The plaintiff in *Mahmood* filed a putative class action against Berbix Inc. for alleged BIPA violations after being required to upload a photo of her driver's license and a "selfie" to rent a car from SilverCar by Audi, which used Berbix's identity verification service.

Another significant BIPA class action involving a third-party vendor is Ronquillo v. Doctor's Assocs., LLC, 2022 U.S. Dist. LEXIS 62730 (N.D. Ill. Apr. 4, 2022). In *Ronquillo*, a Subway restaurant employee alleged that the defendants captured and stored her fingerprints without her informed consent through a point-of-sale system to clock in and out of work and to unlock cash registers. The defendants took the position that they did not actively collect employees' biometric data; rather, at most they merely possessed such data and thus fell outside the scope of BIPA.

The *Ronquillo* court disagreed, finding that the complaint allegations allowed for the reasonable inference that defendants played more than a passive role. 2022 U.S. Dist. LEXIS 62730, at *8. The court also expressly rejected the argument that Section 15(b) did not apply to third-party vendors of technology used by employers to obtain workers' biometric data. This decision deals a significant blow to third-party vendors' efforts to fight BIPA liability, while also demonstrating how courts continue to interpret the statutory text of BIPA in a broad, plaintiff-friendly manner.

Class Certification and Settlement Issues

As noted above, many biometric and AI lawsuits, particularly those involving BIPA, are brought as class actions. However, not all putative class actions can satisfy the rigorous requirement that the class be certifiable. For a class to be certifiable, a class must satisfy all of the requirements of Fed. R. Civ. P. 23(a), and at least one requirement of Rule 23(b). Rule 23(a) requires the following:

- **Numerosity.** The class is so numerous that joinder of all members is impracticable. Fed. R. Civ. P. 23(a)(1).
- **Commonality.** There are questions of law or fact common to the class. Fed. R. Civ. P. 23(a)(2).
- **Typicality.** The claims or defenses of the representative parties are typical of the claims or defenses of the class. Fed. R. Civ. P. 23(a)(3). –and–
- **Adequacy.** The representative parties will fairly and adequately protect the interests of the class. Fed. R. Civ. P. 23(a)(4).

Fed. R. Civ. P. 23(a).

Fed. R. Civ. P. 23(b) requires that a named class representative show that at least one of the following are satisfied:

- Separate actions would result in consistent adjudications or nonparty interests would be substantially impaired. Fed. R. Civ. P. 23(b)(1).
- Final injunctive or declaratory relief is appropriate to the class as a whole. Fed. R. Civ. P. 23(b)(2). –or–
- Common questions of law or fact predominate over any questions affecting only individual members, and a class action is the superior method for adjudicating the controversy. Fed. R. Civ. P. 23(b)(3).

Fed. R. Civ. P. 23(b). Additionally, some jurisdictions impose an additional requirement that the class be administratively feasible, that is, a class definition must be sufficiently definite so that it is administratively feasible for the court to determine whether a particular individual is a member of the proposed class. See Carrera v. Bayer Corp., 727 F.3d 300 (3d Cir. 2013).

As particularly relevant for BIPA class actions which frequently include claims for injunctive relief as well as liquidated damages, the defendants should be mindful that courts should deny motions for class certification under Rule 23(b)(2) when a plaintiff produces no evidentiary proof that injunctive relief is the "primary relief" sought. Leib v. Rex Energy Operating Corp., 2008 U.S. Dist. LEXIS 102847, at *38–40, (S.D. Ill. Dec. 19, 2008) ("Rule 23(b)(2) is invoked in cases where injunctive or declaratory relief is the primary or exclusive relief sought" and "[t]his subsection does not extend to cases in which the appropriate final relief relates exclusively or predominantly to money damages.") (quotation omitted); see also McGlenn v. Driveline Retail Merch., Inc., 2021 U.S. Dist. LEXIS 9532, at *21 (C.D. Ill. Jan. 19, 2021) (declining to certify Rule 23(b)(2) class when "[p]laintiff has not sufficiently shown that a mandatory injunction would remedy the alleged harm," and "[m]oreover, the allegations and arguments indicate that [p]laintiff's main goal is monetary damages").

As the plaintiffs' BIPA claims frequently emphasize requests for monetary damages on behalf of a class, these cases can involve instances where a plaintiff's demand for "monetary relief is not incidental to the injunctive relief." McGlenn, 2021 U.S. Dist. LEXIS 9532, at *21 (citation omitted). Under such circumstances, certification of a Fed. R. Civ. P. 23(b)(2) class would be inappropriate. Additionally, in data privacy litigations, the applicability of an agreement to arbitration can also be a basis for denying class certification.

Notwithstanding these and other potential arguments to oppose class certification, court rulings on motions to certify a class have generally favored plaintiffs. See, e.g., Patel v. Facebook, Inc., 932 F.3d 1264 (9th Cir. 2019).

It is important that practitioners carefully consider the precise contours of the class definition to ensure that the class, as pleaded, is capable of being certified, and incorporate class certification issues as part of forming an overall case strategy. This is particularly so in light of the high stakes associated with litigating biometric and AI claims. As just one example, in August 2022, Snap, the parent company of Snapchat, reached a $35 million settlement in a BIPA putative class action concerning allegations that Snapchat's filters and lenses violated BIPA. With that development, Snap joined a growing list of other companies that have agreed to significant settlements to resolve biometric and AI claims, underscoring the significant litigation risk in this growing space. Other notable settlements include ones involving Facebook ($650 million), TikTok ($92 million), and Google ($100 million).

Recent State Legislation

A number of states recently considered bills regulating the destruction of biometric information collected by entities. States also introduced bills concerning parental rights, children's privacy, and requiring consent for the use of children's biometric information. Some states have tried, and thus far failed, to pass bills restricting the collection, use, and disclosure of biometric information, including:

- **California.** 2021 Bill Text CA S.B. 1038 prohibits law enforcement agencies and officers from using biometric surveillance systems in connection with information connected by body cams.
- **Georgia.** 2021 Bill Text GA S.B. 394 contains many key features of the California Consumer Privacy Act, applicable to biometric information, and requires businesses to obtain consent from consumers prior to collecting personal information.
- **Kentucky.** 2022 Bill Text KY H.B. 626 prohibits the disclosure of "biometric identifiers," collected for a commercial purpose, without the subject's consent except in four narrow circumstances.
- **Maryland.** 2022 Bill Text MD H.B. 259 regulates the use of biometric identifiers, requiring consent for their collection, use, and disclosure, and provides a private right of action.
- **New York.** 2021 Bill Text NY A.B. 680 requires private entities to obtain permission before collecting personal information, including facial biometric information, requires data security measures, and provides for enforcement by the New York Attorney General or by private right of action.

AI Developments

Increased regulatory scrutiny and legislation in the AI space will likely lead to a rise in litigation activity.

Federal Developments with AI

The federal government has recently made advances with using AI and protecting against its potential harms, including the following:

- **Department of Defense (DOD).** The DOD promulgated the DOD Joint All-Domain Command and Control Implementation Plan, which enables the Joint Force to use AI and predictive analytics in battle.
- **Department of Energy (DOE).** The DOE recently established the Inaugural Artificial Intelligence Advancement Council, which will coordinate AI activities in the DOE. The DOE recently issued $10 million to fund AI research on fundamental particles and their interactions.
- **Office of the Director of National Intelligence (ODNI).** In the ODNI, the Intelligence Advanced Research Projects Activity announced the Biometric Recognition & Identification at Altitude and Range program, a research project developing systems to perform whole-body biometric identification from long distances.
- **Internal Revenue Service (IRS).** The IRS abandoned its use of facial recognition technology to authenticate taxpayers' online accounts following bipartisan backlash.
- **National Institute of Standards and Technology (NIST).** NIST released an initial draft of an AI Risk Management Framework and opened it to public comments. It also updated a special publication, Towards a Standard for Identifying and Managing Bias in Artificial Intelligence, which encourages standards for AI to minimize unintentional algorithmic biases.

Recent Federal Legislation

The Algorithmic Accountability Act of 2022, 117 H.R. 6580, proposes to require new transparency and oversight of software, algorithms, and other automated systems. This Act would direct the Federal Trade Commission (FTC) to promulgate regulations requiring covered entities to perform impact assessments and on automated decision-making processes that implicate an "augmented critical decision process" (i.e., that result in any legal or other material effects on a consumer). As of September of 2022, the bill had been referred to the Committee on Commerce, Science, and Transportation. See 117 Bill Tracking S. 3572 for the latest status.

Federal Trade Commission Activity

The FTC has long regulated privacy and security at the federal level, including by enforcing penalties against entities that engage in unfair or deceptive practices regarding consumers' personal data. In recent years, the FTC has aggressively policed the misuse of facial recognition technology.

Several laws play an important role in such enforcement actions:

- Section 5 of the FTC Act, which prohibits unfair or deceptive trade practices
- The Fair Credit Reporting Act (FCRA), which impacts employment, housing, credit, insurance, and other benefits
- The Equal Credit Opportunity Act, which prohibits discrimination against credit applicants

Recent FTC Enforcement Actions

The FTC's enforcement of facial recognition technology and other AI sends a signal to the private sector that care should be exercised in this space. As data privacy concerns more broadly remain a top priority for the agency, additional litigation activity on behalf of regulators is anticipated.

- **Everalbum.** The FTC reached a settlement with Everalbum after it used images from users' accounts to develop facial recognition technology in violation of Section 5(a) of the FTC Act. Everalbum's app allowed users to store photos and videos in a cloud-based storage service. In February 2017, Everalbum launched "Friends," a feature using facial recognition technology, but deceived users when it default-activated said facial recognition technology, which could not be turned off. The settlement required Everalbum to obtain express consent before using facial recognition technology on users' photos and to delete the photos and videos of users who deactivated their accounts and the models and algorithms developed from users' photos and videos.

- **Facebook.** Facebook clashed with the FTC over deceptive facial recognition technology practices. The penalty against Facebook is the largest ever imposed on a company for consumer privacy violations. In part, the FTC alleged that Facebook misled consumers when it told them they could opt in to facial recognition technology despite it being activated by default. As part of the penalty, Facebook was required to provide clear and conspicuous notice of its facial recognition technology and obtain affirmative consent prior to any use materially exceeding prior disclosures.
- **Clarifai.** The FTC opened an investigation against Match Group, after a court granted a motion to dismiss a BIPA lawsuit against Clarifai, Inc., a technology company specializing in AI. The suit alleged that Clarifai violated BIPA by harvesting facial data from OkCupid, a dating site owned by Match. The FTC is investigating whether any entities engaged in unfair or deceptive trade practices in mining data from OkCupid and in using the data in Clarifai's facial recognition technology.
- **WW International, Inc.** The FTC reached a settlement with WW International, Inc. for collecting personal information about underage users without parental consent. As part of the settlement, the company agreed to pay a $1.5 million penalty, delete information from users under age 13, and destroy the related algorithms derived from the data. Moving forward, parents will receive clear and direct notice of the collection and use of their children's information and will be able to consent to such use.

New Commissioner

On May 16, 2022, Alvaro Bedoya was sworn in as the newest FTC commissioner, breaking a months-long deadlock and solidifying a Democratic majority that plans to enact more stringent data privacy protections. Bedoya founded Georgetown Law's Center on Privacy and Technology, where he specialized in issues such as the intersection of privacy and civil rights, biometrics, and children's privacy. In particular, Bedoya has led research into how the government's use of facial recognition technology threatens civil rights.

Advanced Notice of Preliminary Rulemaking

On August 11, 2022, the FTC issued an Advanced Notice of Proposed Rulemaking (ANPR) seeking public comment on "harms stemming from commercial surveillance and whether new rules are needed to protect people's privacy and information."

Recent Congressional Report

On June 16, 2022, the FTC issued a report to Congress regarding the use of AI to combat various online issues including scams, fake reviews, and more serious harms, such as child sexual exploitation. Congress requested the report via the 2021 Appropriations Act.

The report dedicates significant efforts to acknowledging that AI should not be treated as a panacea for the spread of harmful online content, recognizing that "misuse or over-reliance on [AI] tools can lead to poor results that can serve to cause more harm than they mitigate." Such issues include inherent design flaws and inaccuracy in AI resulting from unrepresentative data, faulty algorithms, and lack of context. Bias, discrimination, and invasive surveillance also pose concerns. The report calls for a legal framework to ensure AI does not introduce further harms.

The report offered several recommendations for optimal use of AI. Such recommendations include human intervention to monitor the use of AI, transparency in its use, accountability for entities relying on AI, and imposing responsibility on data scientists and employers for inputs and outputs for AI tools.

Concerns regarding Discrimination in AI

While AI has the potential for widespread societal benefits—increased economic growth, increased productivity, and more—some privacy advocates have expressed concerns regarding its potential unintended discriminatory impact. Such concerns usually stem from either a bias in the algorithm or a bias in the data that the algorithm uses.

Discrimination in Employment

Some privacy advocates have expressed the concern that AI can have unintended discriminatory consequences in employment. Some employers use algorithms to screen potential candidates, which can result in discrimination against underrepresented populations.

In order to address the discriminatory effects of AI in hiring, states and municipalities are passing and proposing legislation to combat these effects. For example, New York City passed a law going into effect in 2023 regulating the use of AI in hiring. Before using AI, employers must audit the tool and ensure it does not create disparate impacts based on race, sex, or ethnicity. The law also creates notice requirements for applicants and employees.

The Algorithmic Accountability Act of 2022, 117 H.R. 6580, would also regulate algorithms in the employment context. If the law goes into effect, it will ban algorithms that produce discriminatory effects based on race, sex, and other characteristics in the context of access to employment. The law would also require employers to audit the algorithms and provide notice to individuals about how their information is used.

Meanwhile, the EEOC is in the early stages of guidance on AI in employment after launching an initiative last year to ensure that algorithms are used fairly in hiring practices. In May 2022, the EEOC issued guidance on algorithms in employment decisions. In particular, the guidance discussed how AI may run afoul of the Americans with Disabilities Act.

Facial Recognition and AI

To some, facial recognition technology poses additional privacy concerns. The FTC has made comments to this effect, noting that it will seek to restrict the use of discriminatory facial recognition software. Former FTC commissioner Rohit Chopra has gone so far as to call facial recognition technology "fundamentally flawed and reinforce[ing] harmful biases." Facial recognition technology can be biased against women and people of color, in part because the developers of such software are largely male and white, and the datasets for these technologies often overrepresent white, male faces.

Artificial intelligence also raises discrimination concerns when it comes to housing and access to medical care. For example, some housing providers use AI systems to screen potential tenants based on court records and other indicators. The FTC has proffered several recommendations for reducing bias in AI. The FTC recommends testing algorithms to make sure they do not discriminate. The FTC also pushes for transparency, encouraging developers to engage in audits, publish the results of audits, and open data to outside inspection.

Current as of: ***09/27/2022***