Volume 7, No. 6 | November–December 2024

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 7, No. 6 | November–December 2024

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. Copyright 2024 Fastcase, Inc. No part of this journal may be reproduced in any form—by microfilm, xerography, or otherwise—or incorporated into any information retrieval system without the written permission of the copyright owner. For customer support, please contact Fastcase, Inc., 729 15th Street, NW, Suite 500, Washington, D.C. 20005, 202.999.4777 (phone), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Leanne Battle
Production Editor: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

This publication is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional services. If legal advice or other expert assistance is required, the services of a competent professional should be sought.

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

729 15th Street, NW, Suite 500, Washington, D.C. 20005
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 729 15th Street, NW, Suite 500, Washington, D.C. 20005.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc.,
26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Leanne Battle, Publisher, Full Court Press at leanne.battle@vlex.com or at
202.999.4777

For questions or Sales and Customer Service:

Customer Service
Available 8 a.m.–8 p.m. Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)

ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Three Best Practices to Mitigate High-Stakes AI Litigation Risk

Justin R. Donoho*

Organizations using artificial intelligence (AI)–based technologies that perform facial recognition or other facial analysis, website advertising, profiling, automated decision making, educational operations, clinical medicine, generative AI, and more increasingly face the risk of being targeted by class action lawsuits and government enforcement actions alleging that they improperly obtained, disclosed, and misused personal data of website visitors, employees, customers, students, patients, and others, or that they infringed copyrights, fixed prices, and more. These disputes often seek millions or billions of dollars against businesses of all sizes. This article identifies recent trends in such varied but similar AI litigation, draws common threads, and discusses three best practices that corporate counsel should consider to mitigate AI litigation risk: (1) add or update arbitration clauses to mitigate the risks of mass arbitration; (2) collaborate with information technology, cybersecurity, and risk/compliance departments and outside advisors to identify and manage AI risks; and (3) update notices to third parties and vendor agreements.

Introduction

Personal data fuels artificial intelligence (AI) and drives today's economy. People disclose their personal data to the internet, businesses, employers, schools, healthcare providers, and other organizations. This personal data feeds AI algorithms' analyses of that data to the profit of companies using the algorithms. In exchange for such data and profits, companies provide free or heavily discounted access to web searching tools, personal email services, news websites, social media, real-time traffic maps, digital assistants, cloud storage, home management systems, human resources technologies, educational technologies, medical diagnostic tools, generative AI, and more. Today's use of AI fueled by personal data is so universally ubiquitous and transformative that scholars agree it has spawned a new age. One plaintiffs' champion calls today the "Age of Surveillance Capitalism."[1] Others call it the "Age of AI."[2]

Regardless of this nomenclature, class actions have proliferated involving AI's allegedly improper use of personal information and other alleged improprieties in a variety of technological areas. This

Robotics, Artificial Intelligence & Law / November–December 2024, Vol. 7, No. 6, pp. 407–428.

ISSN 2575-5633 (print) /ISSN 2575-5617 (online).

article identifies recent trends in such varied types of cases. Next, it draws common lessons from these cases and offers corporate counsel three best practices to mitigate the risk of similar cases. It then briefly concludes.

Recent Trends in High-Stakes Litigation Involving AI Technologies

Facial Analysis and Recognition Technologies

In 2023, plaintiffs filed over 400 class actions alleging that companies improperly obtained individuals' biometric identifiers and biometric information in violation of Illinois' Biometric Information Privacy Act (BIPA). These lawsuits involve large statutory damages, with the top ten BIPA class action settlements in 2023 totaling $147 million.

Some of these BIPA lawsuits have involved AI-based facial recognition systems in which the AI transforms photographs into numerical expressions that can be compared to determine their similarity. These modern systems are in contrast to older, non-AI facial recognition systems in place at the time of BIPA's enactment in 2008, which attempt to identify individuals by using measurements of face geometry that identify distinguishing features of each subject's face. These older systems construct a facial graph from key landmarks such as the corners of the eyes, tip of the nose, corners of the mouth, and chin.

Does BIPA apply to AI machine-learning systems for facial analysis or recognition that do not use facial geometry? Such is the "subject of debate."[3] Decisions issued in 2024 supply mixed rulings in this subject area, suggesting that plaintiffs challenging AI-based facial recognition systems under BIPA sometimes will make it beyond the pleading stage and sometimes will not, but if they do, will have significant hurdles to prove that the technology violates BIPA.

Consider, for example, a popular social media platform's AI-based tag suggestions feature. This feature analyzes photos uploaded by a user to determine whether there is a match with the user's friends. If so, the feature suggests that the user "tag" the friend. Does the feature obtain a "scan of . . . face geometry" in violation of BIPA?[4] This question was addressed in *In Re Facebook Biometric Info. Priv. Litig.*[5] Plaintiffs argued that the technology "necessarily collects scans of face geometry because it uses human facial regions to process, characterize, and ultimately recognize face images."[6] The defendant disagreed, arguing that "the technology has no express dependency on human facial features at all" and instead "learns for itself what distinguishes different faces and then improves itself based on its successes and failures, using unknown criteria that have yielded successful outputs in the past."[7] Both sides submitted expert opinions in support of these arguments on whether the tag suggestion technology performs a scan of face geometry. The district court held: "This is a quintessential dispute of fact for the jury to decide."[8]

The same tag suggestion feature of the same social media company was again analyzed in *Zellmer v. Meta Platforms Inc.*[9] In *Zellmer*, the appellate court explained that the tag suggestion feature works by creating a "face signature," or a "string of numbers that represents a particular image of a face."[10] The feature then compares the face signature with other templates to see if there is a match. As the court further explained, "[n]o one—not even [the defendant, the creator of the face signature]—can reverse-engineer the numbers comprising a given face signature to derive information about a person."[11] For this reason, the court granted summary judgment to the defendant and found the face signature not subject to BIPA because it "cannot identify an individual."[12] The court concluded: "[B]ecause—on the record before us—face signatures cannot identify, they are not biometric identifiers or biometric information as defined by BIPA."[13]

In *Martell v. X Corp.*,[14] the plaintiff alleged that he uploaded a photograph containing his face to the social media platform X (formerly known as Twitter), which X then analyzed for nudity and other inappropriate content using a product called "PhotoDNA." According to the plaintiff, PhotoDNA created a unique digital signature of his face-containing photograph known as a "hash" to compare against the hashes of other photographs, thus necessarily obtaining a "scan of … face geometry" in violation of BIPA. The court rejected this argument and found no plausible allegations of a scan of face geometry because "Plaintiff's Complaint does not include factual allegations about the hashes including that it conducts a face geometry scan of individuals in the photo."[15] Instead, the court found, obtaining a scan of face geometry means "zero[ing] in on [a face's] unique contours to create a 'template' that maps and records [the individual's] distinct facial measurements."[16] In short, the Illinois court found on the pleadings that there were no plausible allegations that an AI-based facial recognition system violated BIPA—on the same ground that AI-based facial recognition systems do not involve face geometry that the California court found was a ground only a jury could decide *In re Facebook*.

A factor favoring X Corp. in *Martell* was that, unlike the face-tagging feature in *In re Facebook* and *Zellmer*, "PhotoDNA is not facial recognition software."[17] As the court explained, "Plaintiff does not allege that the hash process takes a scan of face geometry, rather he summarily concludes that it must. The Court cannot accept such conclusions as facts adequate to state a plausible claim."[18] In other cases in which plaintiffs have brought BIPA claims involving facial analysis technologies performing functions other than facial recognition, companies have received mixed rulings when challenging the plausibility of allegations that their technologies obtained facial data "biologically unique to the individual."[19] BIPA defendants have been similarly successful at the pleading stage as X Corp., for example, in securing dismissal of BIPA lawsuits involving virtual try-on technologies that allow customers to use their computers to visualize glasses, makeup, or other accessories on their face.[20]

Defendants have been less successful at the pleading stage and continue to litigate their cases, however, in cases involving software verifying compliance with U.S. passport photo requirements;[21] software analyzing facial expressions of salespeople to generate feedback about their "elevator pitch";[22] and software detecting fever from the forehead and whether the patient is wearing a face mask.[23] *Martell* bolsters these mixed rulings in non–facial recognition cases in favor of the defendants, with its finding that mere allegations of verification that a face-containing picture is not pornographic are insufficient to establish that the defendant obtained any biometric identifier or biometric information.

While undoubtedly litigation over BIPA will continue regarding AI-based facial analysis and recognition technologies, the *Zellmer* and *Martell* decisions supply useful precedent for companies facing high-stakes BIPA lawsuits containing insufficient allegations that they have obtained a scan of facial geometry unique to an individual.

Website Advertising Technologies

In 2023, plaintiffs filed over 250 class actions alleging that Meta Pixel, Google Analytics, and other similar software embedded in defendants' websites secretly captured plaintiffs' web browsing data and sent it to Meta, Google, and other online advertising agencies. This software, often called "website advertising technologies" or "adtech," is a common feature on many websites in operation today; millions of companies and governmental organizations utilize it.[24] Adtech works by collecting information about a person's web-browsing behavior and utilizing AI to analyze the collected data and serve targeted advertisements based on the analysis.

In these lawsuits, plaintiffs generally allege that the defendant organization's use of adtech violated federal and state wiretap statutes, consumer fraud statutes, and other laws, and they often seek hundreds of millions of dollars in statutory damages. Plaintiffs have focused the bulk of their efforts to date on healthcare providers, but they have filed suits that span nearly every industry, including retailers, consumer products, and universities. Several of these cases have resulted in multimillion-dollar settlements, several have been dismissed, and the majority remain undecided.

Illustrative in this area are various cases decided in 2024 that reached mixed results. In *Smart v. Main Line Health Inc.*,[25] the U.S. District Court for the Eastern District of Pennsylvania dismissed in its entirety a class action complaint alleging that a nonprofit health system's use of website advertising technology disclosed the plaintiff's individually identifiable health information (IIHI) in violation of the Federal Wiretap Act and in commission of the common-law torts of negligence and invasion of privacy. To state a claim for violation of the Electronic Communications Privacy Act (ECPA), also known as the Federal Wiretap Act, a plaintiff must show an intentional interception of the contents of an electronic communication using a device.[26] The ECPA is a one-party consent statute, meaning that there is no liability under the statute for any party to the communication "unless such communication is intercepted for the purposes of committing a criminal or tortious act in violation of the Constitution or laws of the United States or any State."[27]

The plaintiff argued that he plausibly alleged the health system's criminal or tortious purpose because, under the Health Insurance Portability and Accountability Act (HIPAA), it is a federal crime for a healthcare provider to knowingly disclose IIHI to another person. The district court rejected this argument, finding the plaintiff failed to allege sufficient facts to support an inference that the health system disclosed his IIHI. As the district court explained:

"Plaintiff has not alleged which specific web pages he clicked on for his medical condition or his history of treatment with Main Line Health."[28] In short, the district court concluded that the plaintiff's failure to sufficiently allege IIHI was reason alone for the court to dismiss the plaintiff's ECPA claim. On the plaintiff's remaining claims, the district court held that lack of sufficiently pled IIHI defeated the causation element of the plaintiff's negligence claim and defeated the element of the plaintiff's invasion of privacy claim that any intrusion must have been "highly offensive to a reasonable person."[29] The *Smart* decision is significant because it shows that such claims cannot surmount Rule 12(b)(6)'s plausibility standard without specifying the information allegedly disclosed.

In *Nienaber v. Overlake Hosp. Med. Ctr.*,[30] the U.S. District Court for the Western District of Washington dismissed in its entirety a class action complaint alleging that a nonprofit healthcare organization's use of adtech violated the Federal Wiretap Act. The district court dismissed the ECPA claim because "Plaintiff fails to plead a tortious or criminal use of the acquired communications, separate from the recording, interception, or transmission."[31] As the court explained, "Courts within this Circuit have held 'that a plaintiff must plead sufficient facts to support an inference that the offender intercepted the communication for the purpose of a tortious or criminal act that is *independent* of the intentional act of recording or interception itself.'"[32] The court also dismissed the plaintiff's negligence claim due to insufficiently alleged disclosure of IIHI,[33] invasion of privacy claim due to lack of any alleged intrusion or publicity,[34] breach of implied contract claim due to lack of plausibly alleged mutual assent and damages,[35] and other claims for similar and additional reasons.[36]

In *Kane v. Univ. of Rochester*,[37] a New York district court found that the adtech plaintiffs sufficiently alleged their IIHI entered on the defendant's website in the form of alleged appointment scheduling information identifying the user who scheduled the appointment, the provider, and the provider's specialty.[38] Therefore, the court found the plaintiffs plausibly alleged a purpose of disclosing IIHI in violation of HIPAA sufficient to invoke the crime-tort exception to a party's non-liability under ECPA.[39] Thus, the court acknowledged, it joined the "[a]t least one [other] district court" finding an adtech plaintiff sufficiently invoked the crime-tort exception under ECPA with allegations that the website owner's purpose was to "enhance its marketing efforts."[40] In addition to the

ECPA claim, the district court also declined to dismiss plaintiffs' claims for breach of express contract, unjust enrichment, bailment, and violation of New York's deceptive trade practices statute.[41]

In many adtech cases, claims under the Federal Wiretap Act (ECPA) and state wiretap acts are the highest value dollar claims by far due to the statutory damages they seek per claim multiplied by numbers of website visitors, often totaling into the hundreds of millions or billions of dollars. Notably, neither *Smart* nor *Kane* addressed other reasons that may have required dismissal of the plaintiffs' ECPA claims, such as (1) lack of criminal or tortious intent even if IIHI had been sufficiently alleged,[42] and (2) lack of any interception.[43]

The legal landscape in this area has only begun to develop under many plaintiffs' theories of liability, statutes, common laws, and theories of multimillion- and billion-dollar damages. Key adtech cases to watch with potential upcoming rulings include cases involving issues relating to the purported application of wiretap laws to adtech, class certification, and federal jurisdiction.

Profiling and Automated Decision-Making Technologies

Statutes enacted in the past two years in California, Colorado, Connecticut, and Virginia address consumers' rights to opt out of companies' use of profiling technologies that use personal data to make automated decisions resulting in the provision or denial of financial or lending services, housing, insurance, education enrollment opportunity, criminal justice, employment opportunities, healthcare services, or access to essential goods and services.[44]

Although the statutory landscape specific to profiling and automated decision-making technologies is only recently emerging, courts have issued a few recent decisions in cases alleging improper use of profiling technologies under older statutes regarding employment discrimination, lie detection, and consumer protection. These cases raise significant implications for any company using profiling technologies today and provide a preview of the types of risks such companies may face in the future as additional states enact or amend their data privacy statutes to address profiling and automated decision-making technologies. As described below, these risks include governmental enforcement actions, class actions, and associated remedies, including a relatively new and impactful one being pursued by the Federal Trade Commission (FTC) in the form of algorithmic disgorgement.

In a first for the U.S. Equal Employment Opportunity Commission (EEOC) and the issue of AI, last year the EEOC filed a joint settlement agreement in *EEOC v. iTutorGroup Inc.*[45] The resulting consent decree memorialized a $365,000 settlement between the EEOC and a tutoring company for claims under the Age Discrimination and Employment Act (ADEA) involving hiring software that automatically rejected applicants based on their age.[46] This unprecedented result culminated from the EEOC's Artificial Intelligence and Algorithmic Fairness Initiative launched in 2021 to ensure that profiling technologies do not become a high-tech pathway to discrimination.[47]

The EEOC's activities concerning profiling technologies making automated employment decisions continues in 2024. In *Mobley v. Workday Inc.*,[48] an African-American male over the age of 40 with anxiety and depression, brought a class action lawsuit alleging that he applied to 80 to 100 jobs with companies that use Workday's screening tools. Despite holding a bachelor's degree in finance and an associate's degree in network systems administration, the plaintiff claimed he did not receive a single job offer.[49] The plaintiff alleged class claims under Title VII, the ADEA, and the Americans with Disabilities Act.[50] Workday moved to dismiss and the court granted Workday's motion on the basis that Workday, a technology company, could not be held liable as an "employment agency" under the antidiscrimination statutes at issue.[51] However, the court granted the plaintiff leave to amend his complaint on the issue of whether Workday could be held liable, alternatively, as an "indirect employer" or "agent."[52] The plaintiff amended his complaint and, thereafter, the EEOC filed an amicus brief arguing that the plaintiff's amended complaint plausibly alleged that Workday is an employment agency, indirect employer, and agent of employers.[53] Thereafter, the court held that the plaintiff sufficiently alleged that Workday was an agent for employers since it made employment decisions in the screening process through the use of artificial intelligence.[54] This decision likely will be used as a roadmap for the plaintiffs' bar to bring discrimination claims against third-party vendors involved in the employment decision process, especially those using algorithmic software to make those decisions. Companies should also take heed, especially given the EEOC's prior guidance that suggests employers should be auditing their vendors for the impact of their use of artificial intelligence

In *Baker v. CVS Health Corp.*,[55] the plaintiff brought a claim under Massachusetts' Lie Detector Statute,[56] alleging that his prospective employer used video-interview technology to analyze his facial expressions, eye contact, voice intonation, and inflection using AI. The AI then conveyed its findings to the prospective employer "with a numerical employability score or competency-level scoring report" to "detect whether an applicant has an innate sense of integrity and honor, help with lie detection and screen out embellishers, and organize applicant competencies including reliability, honesty, and integrity."[57] The plaintiff moved to dismiss, arguing lack of standing and no private right of action to enforce the statute's notice provision. The court denied the motion, finding that the plaintiff "pleaded a concrete informational injury. . . . Although the notice would not have specifically informed [plaintiff] that the [i]nterview was a lie detector test, it would have primed him to view the interview more critically. [Plaintiff]'s injury is of the kind the statute was designed to protect."[58] The court also found a private right of action to enforce the notice provision under the express language of the statute.[59]

In *FTC v. Rite Aid Corp.*,[60] the FTC brought an enforcement action against a retailer alleging that it deployed facial recognition and automated decision-making technology in its retail stores to identify individuals it had previously deemed likely to engage in shoplifting or other criminal behavior. According to the FTC, the retailer's use of profiling technology was an unfair practice under Section 5 of the Federal Trade Commission Act,[61] because, among other things, it was especially likely to result in false-positive matches for Black, Latino, Asian, and women consumers.[62] The district court entered a stipulated order for permanent injunction and other relief to resolve all matters in dispute arising from the complaint. The order, among other things, required the retailer to delete all photos and videos it had obtained and "any data, models, or algorithms derived in whole or in part therefrom."[63] Thus, the FTC continued its latest trend of wielding algorithmic disgorgement as an enforcement tool.[64] If applied against AI-based deep-learning systems that have become available in recent years, algorithmic disgorgement as a litigation remedy could have far-reaching effects on AI adoption strategies. In short, getting legal compliance at the start of an algorithm's deep-learning process is essential to avoid the risk of a court-ordered do-over of all that deep learning.

In 2024 plaintiffs filed amendments to their class action complaints against three health insurers alleging that the insurers' AI-based automated decision-making technologies known as PxDx and nH Predict improperly rejected claims for health insurance without sufficient human oversight in breach of contract and violation of deceptive and unfair practices statutes and other laws.[65] Do PxDx and nH Predict use personal data and profiling to make their algorithmic decisions? Such cannot be determined, according to four healthcare researchers with doctoral degrees.[66] Regardless of the actual underlying algorithmic logic of these algorithms, these cases illustrate that even if consumers cannot articulate the underlying logic of an algorithm making automated decisions producing legal or similarly significant effects, companies utilizing such algorithms risk facing class action lawsuits if the algorithm's output is perceived as unfair.

Companies that use or make AI-based profiling technologies to automate significant decisions would be wise to pay attention to this latest trend of cases involving such technologies. As illustrated, new laws regulating such technologies are just being enacted and are on the horizon; the EEOC, FTC, and plaintiffs' bar are active in this space; and a new remedy of algorithmic disgorgement being pursued by the FTC could have serious business impacts.

Other AI-Based Technologies

Dozens of AI class actions have been filed in the past two years involving AI technologies that perform educational operations, clinical medicine, pricing in purported violation of antitrust laws, generative AI in alleged violation of copyright, wiretapping, data privacy, and other laws, recognition of other bodily characteristics besides faces, and more. Although there have been relatively few decisions issued in any one of these additional categories of technologies, two stand out as having significant implications for AI class actions of all types.

In *Dinerstein v. Google LLC*,[67] a patient at a university hospital alleged claims arising from a research collaboration between Google and the university whereby the partners aspired to "[h]arness[] the power of artificial intelligence" to improve patients' healthcare outcomes.[68] To do this, the university supplied several years of anonymized patient medical records to train Google's AI algorithms.[69] The plaintiff filed a class action against Google and the university, alleging his anonymized records were included in the algorithmic training effort entitling him to damages under various common-law theories.

The U.S. Court of Appeals for the Seventh Circuit ruled that the plaintiff lacked standing to bring his lawsuit for several reasons.

First, the court found no past harm because the patient data training the algorithm had been sufficiently anonymized.[70] Second, the court found no imminent risk of future harm because any threat of reidentification was "wholly speculative and implausible."[71] Third, the court rejected the plaintiff's theory that he overpaid the university for data privacy and did not receive data privacy in return, finding it implausible that he would not have paid for medical services had he known his anonymized medical information would be used for research.[72] Finally, the court rejected the plaintiff's theory that the university underpaid him for an interest in his medical records because under Illinois law medical records belong to the medical provider and, moreover, the university's use of the plaintiff's medical information did not deprive him of its economic value.[73]

Dinerstein is a win for defendants of class actions based on AI-based algorithms causing no harm. In such cases, the *Dinerstein* decision can be cited as useful precedent for rejecting plaintiffs' damages theories of insufficient anonymization, risk of reidentification, overpayment, and underpayment. Moreover, plaintiffs' damages theories were rejected in *Dinerstein* in major part because the plaintiffs failed to plausibly allege that the university failed to perform a "typical de-identification process."[74] What constitutes a typical de-identification process is a fast-evolving topic as AI reidentification algorithms become smarter. Recognizing this concern in his Executive Order on AI, President Biden ordered research and development into privacy-enhancing technologies and the creation of new guidelines "[t]o mitigate privacy risks potentially exacerbated by AI—including by AI's facilitation of the collection or use of information about individuals, or the making of inferences about individuals."[75] *Dinerstein*'s holding may remain applicable to companies whose "typical de-identification process" keeps up with evolving privacy standards stemming from the Executive Order on AI.

Another case with impact across AI technologies is *Tremblay v. OpenAI Inc.*[76] In *Tremblay*, the plaintiffs (a group of authors) alleged that an AI company trained its algorithm by "copying massive amounts of text" to enable it to "emit convincingly naturalistic text outputs in response to user prompts."[77] The plaintiffs alleged these outputs included summaries that were so accurate that the algorithm must have retained knowledge of the ingested copyrighted works in order to output similar textual content.[78] An exhibit to the complaint displaying the algorithm's prompts and outputs purported to support these allegations.[79]

The AI company sought discovery of (1) the account settings, and (2) the algorithm's prompts and outputs that "did not" include the plaintiffs' "preferred, cherry-picked" results.[80] The plaintiffs refused, citing work-product privilege, which protects from discovery documents prepared in anticipation of litigation or for trial. The AI company argued that the authors waived that protection by revealing their preferred prompts and outputs, and asked the court to order production of the negative prompts and outputs, too, and all related account settings.[81]

The court agreed with the AI company and ordered production of the account settings and all of the plaintiffs' pre-suit algorithmic testing results, including any negative ones, for four reasons. First, the court held that the algorithmic testing results were not work product but "more in the nature of bare facts."[82] Second, the court determined that "even assuming arguendo" that the work-product privilege applied, the privilege was waived "by placing a large subset of these facts in the [complaint]."[83] Third, the court reasoned that the negative testing results were relevant to the AI company's defenses, notwithstanding the plaintiffs' argument that the negative testing results were irrelevant to their claims.[84] Finally, the court rejected the plaintiffs' argument that the AI company can simply interrogate the algorithm itself. As the court explained, "without knowing the account settings used by Plaintiffs to generate their positive and negative results, and without knowing the exact formulation of the prompts used to generate Plaintiffs' negative results, Defendants would be unable to replicate the same results."[85]

Tremblay is a win for defendants of class actions based on alleged outputs of AI-based algorithms. In such cases, the *Tremblay* decision can be cited as useful precedent for seeking discovery from recalcitrant plaintiffs of all of plaintiffs' pre-suit prompts and outputs, and all related account settings. The court's fourfold reasoning in *Tremblay* applies not only in generative AI cases but also other AI cases. For example, in adtech cases, plaintiffs should not be able to withhold their adtech settings (the account settings), their browsing histories and behaviors (the prompts), and all documents relating to targeted advertising they allegedly received as a result, any related purchases, and alleged damages (the outputs).

As AI-related technologies continue their growth spurt, and litigation in this area spurts accordingly, the implications of *Dinerstein* and *Tremblay* may reach far and wide.

Best Practices to Mitigate AI Litigation Risk

Add or Update Arbitration Agreements to Mitigate the Risks of Mass Arbitration

Many organizations have long been familiar with the strategy of deterring class and collective actions by presenting arbitration clauses containing class and collective action waivers prominently for web users, consumers, and employees to accept via click wrap, browse wrap, login wrap, shrink wrap, and signatures. Such agreements would require all allegedly injured parties to file individual arbitrations in lieu of any class or collective action. Moreover, the strategy goes, filing hundreds, thousands, or more individual arbitrations would be cost-prohibitive for so many putative plaintiffs and thus deter them from taking any action against the organization in most cases.

Over the past decade, this strategy of deterrence was effective.[86] Times have changed. Now enterprising plaintiffs' attorneys with burgeoning war chests, litigation funders, and high-dollar novel claims for statutory damages are increasingly using mass arbitration to pressure organizations into agreeing to multimillion-dollar settlements, just to avoid the arbitration costs. In mass arbitrations filed with the American Arbitration Association (AAA) or Judicial Arbitration and Mediation Services (JAMS), for example, fees can total millions of dollars just to defend only 500 individual arbitrations.[87] One study found up-front fees ranging into the tens of millions of dollars for some large mass arbitrations.[88] Companies with old arbitration clauses have been caught off guard with mass arbitrations and have sought relief from courts to avoid having to defend these mass arbitrations, and this relief was rejected in several recent decisions where the court ordered the defendant to arbitrate and pay the required hefty mass arbitration fees.[89]

If your organization has an arbitration clause, then one of the first challenges for counsel defending many newly served class action lawsuits these days is determining whether to move to compel arbitration. Although it could defeat the class action, is it worth the risk of mass arbitration and the potential projected costs of mass arbitration involved? Sometimes not.

Increasingly organizations are mitigating this risk by including mechanisms in their arbitration agreements to deter mass arbitrations and streamline any mass arbitration process. Such mechanisms often include reference to and consideration of the latest applicable mass arbitration rules,[90] a pre-dispute informal resolution clause, and a mass arbitration protocol, including provisions for bellwether proceedings, mediation, escape hatch to return to court, staging of subsequent bellwether proceedings, streamlined discovery, and more.

This area of the law is developing quickly. In one recent case, the Seventh Circuit reversed a district court's order requiring a BIPA defendant to pay over $4 million in initial mass arbitration filing fees where the AAA, accordingly, terminated the proceedings.[91] As the Seventh Circuit explained, at that point, the arbitration was complete.[92] Thus, the consumers could not compel the BIPA defendant to pay the mass arbitration fees but were free to pursue their claims in district court.[93] The *Wallrich* ruling does not enable defendants without mass arbitration provisions to escape mass arbitration by just not paying initial mass arbitration filing fees, however. As the Seventh Circuit explained, plaintiffs may advance arbitration initiation fees themselves, thus leaving the door open for plaintiffs to attempt to recoup those fees as the arbitrations proceed.[94] Moreover, following *Wallrich*, it remains to be seen how arbitration tribunals will proceed in this fast-developing area. Instead of terminating the arbitration proceedings when mass arbitration defendants refuse to pay hefty initiation fees, in the future arbitration tribunals have an alternative path to obtain their fees, which the Seventh Circuit described as: "stay[] the case or threaten[] to decline administering future consumer arbitrations with [the defendant]."[95] In short, companies should protect themselves with mass arbitration provisions notwithstanding this ruling in order to minimize risks associated with mass arbitrations.

Collaborate with Information Technology, Cybersecurity, and Risk/Compliance Departments and Outside Advisors to Identify and Manage AI Risks

Beyond the relatively simple but crucial task of updating arbitration agreements, another of corporate counsel's main imperatives to mitigate AI litigation risk is to ensure that all AI software, networks, and hardware the company uses are in compliance with a wide variety of laws often alleged as being violated in plaintiffs' AI-related class action complaints. These laws include biometric privacy statutes, wiretap statutes, unfair and deceptive practices statutes, antidiscrimination statutes, copyright statutes, antitrust statutes, and other statutes that provide for high-dollar statutory damages. AI class action plaintiffs also often raise theories of actual damages and seek injunctive relief under these statutes and under a number of common-law claims, including claims for invasion of privacy, breach of contract, negligence, and the commission of other common-law torts.

The first step in ensuring compliance of AI software, networks, and hardware with all these laws is to identify all the AI software, networks, and hardware.

For example, does your company know what adtech is present on its public-facing websites? It could have been installed on a website by a vendor without proper authorization, or as a default without any human intent by using some web publishing tools. If so, did your company's processes and technologies capture that change to its information technology (IT) environment?

More generally, does your company have processes and technologies in place to capture AI hardware, software, and network inventory information whenever the company adds and updates business activities, changes business structure, changes its external business ecosystem, and experiences changes resulting from the conduct of ongoing business activities?

Check with your IT and cybersecurity departments and, as needed, any outside specialists such as adtech auditors. All of these types of individuals are often involved in continuously capturing inventory information about IT software, networks, and hardware, including those that power the company's use of AI, such that corporate counsel should collaborate with them as follows:

- *Collaborate with the IT Department.* IT inventory capture is typically a major activity performed by IT departments as part of IT service management practices, including maintenance of a configuration management database (CMDB) and an IT service catalog.[96]
- *Collaborate with the Cybersecurity Department.* IT inventory capture is typically a major activity performed by cybersecurity departments as part of identifying and managing cyber risks.[97]
- *Collaborate with Outside Specialists Such as Adtech Auditors.* IT inventory capture is often performed by specialist outside auditors. For example, organizations should consider whether to have an audit performed before any litigation arises as to which adtech is or has been installed on which

web pages when and which data types were transmitted as a result. Multiple experts specialize in such adtech audits and serve as expert witnesses should any adtech litigation arise.

Only as AI inventory is identified can its associated risk be managed.

Managing AI litigation risk may include the following activities:

- *Collaborate with the Risk/Compliance Department*. Often management of any type of litigation risk is performed as part of an overall enterprise risk management (ERM) program by a company's risk/compliance department. ERM programs manage a wide variety of risks under a unified program, including managing litigation risks, risks to customer service, cybersecurity risks, the risks of being underinsured, and other risks.[98] AI poses its own unique risks, giving rise to AI risk management frameworks that may also be integrated in your company's ERM program.[99]
- *Collaborate with In-House and Outside Attorneys*. This article endeavored to highlight recent trends in high-stakes litigation involving AI technologies so as to assist corporate counsel in identifying risk associated with AI litigation that the company may be facing now and may face in the future. Those AI litigation trends are accelerating and multiplying and need to be continually monitored accordingly. Attorneys who monitor such trends may be helpful in:
  - Litigating such cases effectively and efficiently, as the need for any litigation arises;
  - Advising on updating arbitration agreements to mitigate the risk of mass arbitration;
  - Providing legal advice in connection with adtech audits; and
  - Advising on updating and modernizing website terms of use, data privacy policies, and vendor agreements (next topic).

Update Notices to Third Parties and Vendor Agreements

Organizations should consider whether to modify their website terms of use, data privacy policies, telephonic notices, and all other notices to the organizations' website visitors, callers, physical visitors, customers, employees, students, and patients, to describe the organization's use of AI in additional detail. Doing so could deter or help defend a future AI class action lawsuit similar to the many that are being filed today, alleging omission of such additional details, raising claims brought under various states' wiretap acts and consumer fraud acts, and seeking multimillion-dollar and billion-dollar statutory damages.

Organizations should consider adding to contracts with vendors clauses prohibiting the vendor from incorporating any unwanted AI into the organization's systems and processes. For example, in contracts with website vendors and marketing vendors, consider adding clauses that prohibit the vendor from incorporating any unwanted adtech into the organization's public-facing websites. As another example, in contracts with staffing agencies of temporary employees, consider adding clauses that prohibit the vendor from obtaining biometric identifiers and biometric information without the temporary employee's consent. In short, adding such prohibitory clauses could help disprove the element of intent at issue in many claims brought under the recent explosion of AI lawsuits.

Conclusion

This article identified recent trends in high-stakes litigation involving AI technologies, including facial analysis and recognition, adtech, profiling, automated decision making, and other AI technologies. It described how these trends show that companies using these various AI technologies may face multimillion- or billion-dollar risks of litigation seeking statutory and common-law damages under a wide variety of laws, including BIPA, wiretap statutes, unfair and deceptive practices statutes, antidiscrimination statutes, copyright statutes, antitrust statutes, common-law invasion of privacy, breach of contract, negligence, and more.

Finally, it described three best practices companies can follow to mitigate this AI litigation risk:

1. Add or update arbitration agreements to mitigate the risks of mass arbitration;
2. Collaborate with IT, cybersecurity, and risk/compliance departments, and outside advisors to identify and manage AI risks; and
3. Update notices to third parties and vendor agreements.

Notes

* Justin Donoho, special counsel in the Chicago office of Duane Morris LLP, may be contacted at jrdonoho@duanemorris.com.

[1] See Shoshana Zuboff, The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power (2019). Cited by plaintiffs in, e.g., Shanahan v. IXL Learning Inc., No. 24-CV-2724, ECF No. 1 at 9 (N.D. Cal. May 7, 2024); Cherkin v. PowerSchool Holdings Inc., No. 24-CV-2706, ECF No. 1 at 5 (N.D. Cal. May 6, 2024); Louth v. NFL Enters. LLC, No. 21-CV-405, ECF No. 14 at 11 (D. R.I. Jan. 3, 2022).

[2] See Henry A. Kissinger, Eric Schmidt, and Daniel Huttenlocher, The Age of AI and Our Human Future (2021) (opining that the Age of AI follows the Age of Reason).

[3] "The Sedona Conference U.S. Biometric Systems Privacy Primer," The Sedona Conference Journal, vol. 25, at 200 (May 2024).

[4] 740 ILCS 14/10.

[5] In Re Facebook Biometric Info. Priv. Litig., 2018 WL 2197546 (N.D. Cal. May 14, 2018).

[6] Id. at *2.

[7] Id.

[8] Id. at *3.

[9] Zellmer v. Meta Platforms Inc., 2024 WL 3016946 (9th Cir. June 17, 2024).

[10] Id. at *2.

[11] Id.

[12] Id. at *4.

[13] Id. at *7.

[14] Martell v. X Corp., 2024 WL 3011353 (N.D. Ill. June 13, 2024).

[15] Martell, supra n.13, at *3.

[16] Id.

[17] Id. at *2.

[18] Id. at *3.

[19] 740 ILCS 14/5(c).

[20] See Clarke v. Aveda Corp., 2023 WL 9119927, at *2 (N.D. Ill. Dec. 1, 2023); Castelaz v. Estee Lauder Cos. Inc., 2024 WL 136872, at *7 (N.D. Ill. Jan. 10, 2024).

[21] Daichendt v. CVS Pharmacy Inc., 2023 WL 3559669, at *2 (N.D. Ill. May 4, 2023).

[22] Clark v. Microsoft Corp., 688 F. Supp. 3d 743, 745 (N.D. Ill. 2023).

[23] Trio v. Turing Video Inc., 2022 WL 4466050, at *13 (N.D. Ill. Sept. 26, 2022).

[24] See, e.g., Customer Data Platform Institute, "Trackers and Pixels Feeding Data Broker Stores" (reporting that "47% of websites using Meta Pixel, including 55% of S&P 500, 58% of retail, 42% of financial, and 33% of health-

care"), https://www.cdpinstitute.org/news/trackers-and-pixels-feeding-data-broker-data-stores; BuiltWith, "Facebook Pixel Usage Statistics" (offering access to data on over 14 million websites using the Meta Pixel and stating, "We know of 6,343,733 live websites using Facebook Pixel and an additional 8,185,233 sites that used Facebook Pixel historically and 2,826,894 websites in the United States"), https://trends.builtwith.com/analytics/Facebook-Pixel.

[25] Smart v. Main Line Health Inc., 2024 WL 2943760 (E.D. Pa. June 10, 2024).

[26] Id. at *3.

[27] Id. (quoting 18 U.S.C. § 2511(2)(d)); 18 U.S.C. § 2511(2)(d).

[28] Id. at 3 (collecting cases).

[29] Main Line, 2024 WL 2943760, at *4.

[30] Nienaber v. Overlake Hosp. Med. Ctr., 2024 WL 2133709 (W.D. Wash. May 13, 2024).

[31] Id. at *15.

[32] Id. (emphasis in original).

[33] Id. at **7-9.

[34] Id. at **9-10.

[35] Id. at **11-13.

[36] Id. at *18.

[37] Kane v. Univ. of Rochester, 2024 WL 1178340, at *5 (W.D.N.Y. Mar. 19, 2024).

[38] Id. at **5-7.

[39] Id. at **7-8.

[40] Id. at *7.

[41] Id. at *18.

[42] See, e.g., Nienaber, 2024 WL 2133709, at *15 (dismissing wiretap claim because "Plaintiff fails to plead a tortious or criminal use of the acquired communications, separate from the recording, interception, or transmission"); Katz-Lacabe v. Oracle Am. Inc., 668 F. Supp. 3d 928, 945 (N.D. Cal. 2023) (dismissing wiretap claim because defendant's "purpose has plainly not been to perpetuate torts on millions of Internet users, but to make money").

[43] See, e.g., Allen v. Novant Health Inc., 2023 WL 5486240, at *4 (M.D.N.C. Aug. 24, 2023) (dismissing wiretap claim because an intended recipient cannot "intercept"); Glob. Pol'y Partners, LLC v. Yessin, 686 F. Supp. 2d 631, 638 (E.D. Va. 2009) (dismissing wiretap claim because the communication was sent as a different communication, not "intercepted").

[44] See Cal. Civ. Code § 1798.185 (regulations forthcoming); Colo. Rev. Stat. §§ 6-1-1303(10), 6-1-1306(1)(a)(I)(C); Conn. Gen. Stat. §§ 42-515(15), 42-518(a)(5)(C); Va. Code §§ 59.1-575, 59.1-575(A)(5)(iii); see also NYC Admin. Code §§ 20-870 to -874 (limiting use of automated employment decision tools).

[45] EEOC v. iTutorGroup Inc., No. 22-CV-2565 (E.D.N.Y. Aug. 9, 2023).

[46] Id., 2023 WL 6261089.

47. See Alex W. Karasik, "An Examination of the EEOC's Artificial Intelligence Revolution," The Brief, vol. 53, no. 2 (June 2024).

48. Mobley v. Workday Inc., 2024 WL 208529 (N.D. Cal. Jan. 19, 2024).

49. Id. at *1.

50. Id. at *2.

51. Id. at **5-6.

52. Id.

53. Id., No. 23-CV-770, ECF No. 60-1.

54. Mobley v. Workday, Inc., 2024 WL 3409146 (N.D. Cal. July 12, 2024).

55. Baker v. CVS Health Corp., 2024 WL 655949 (D. Mass. Feb. 16, 2024).

56. Mass. Gen. Laws ch. 149 § 19.

57. Baker, supra n. 52 at *2 (cleaned up).

58. Id. at *3.

59. Id.

60. FTC v. Rite Aid Corp., No. 23-CV-5023 (E.D. Pa.).

61. 15 U.S.C. §§ 45(a), (n).

62. ECF No. 1 ¶ 86.

63. ECF No. 19 at 13 (Feb. 26, 2024).

64. See Joshua A. Goland, Algorithmic Disgorgement: Destruction of Artificial Intelligence Models As the FTC's Newest Enforcement Tool for Bad Data, 29 Rich. J.L. & Tech. 1, 2 (2023).

65. Lokken v. UnitedHealth Grp. Inc., No. 23 CV-3514 (D. Minn. first amended complaint filed 4/5/24); Barrows v. Humana Inc., No. 23-CV-654 (W.D. Ky. first amended complaint filed 4/22/24); Kisting-Leung v. Cigna Corp., No. 23-CV-1477 (E.D. Cal. third amended complaint filed June 14, 2024).

66. See Rachele Hendricks-Sturrup Joe Vandigo Christina Silcox Elisabeth M. Oehrlein, "Best Practices for AI in Health Insurance Claims Adjudication and Decision-Making," Health Affairs (June 20, 2024) ("Transparency is lacking.... It is unclear whether or how such algorithms [PxDx and nH Predict] were built... may be biased due to the underrepresentation of certain US demographic populations and subpopulations in data used to train the algorithms"), https://www.healthaffairs.org/content/forefront/best-practices-ai-health-insurance-claims-adjudication-and-decision-making.

67. Dinerstein v. Google, LLC, 73 F.4th 502 (7th Cir. 2023).

68. Id. at 507.

69. Id.

70. Id. at 513-14.

71. Id. at 514-16.

72. Id. at 517-18.

73. Id. at 518.

74. Id. at 514.

75. Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence § 9 (Oct. 30, 2023) (Executive Order on AI).

[76] Tremblay v. OpenAI Inc., No. 23-CV-3223 (N.D. Cal. June 13, 2024).

[77] Id. at 1.

[78] Id. at 2.

[79] Id.

[80] Id. (emphasis omitted).

[81] Id. at 2-3.

[82] Id. at 5-6.

[83] Id. at 6.

[84] Id. at 6.

[85] Id.

[86] In 2015, for example, a large study found that of 33 banks that had engaged in practices relating to debit card overdrafts, 18 endured class actions and ended up paying out $1 billion to 29 million customers, whereas 15 had arbitration clauses and did not endure any class actions. See Consumer Protection Financial Bureau, Arbitration Study: Report to Congress, Pursuant to Dodd-Frank Wall Street Reform and Consumer Protection Act § 1028(a) at Section 8, https://files.consumerfinance.gov/f/201503_cfpb_arbitration-study-report-to-congress-2015.pdf. These 15 with arbitration clauses paid almost nothing—less than 30 debit card customers per year in the entire nation filed any sort of arbitration dispute regarding their cards during the relevant timeframe. See id. at Section 5, Table 1. Another study of AT&T from 2003 to 2014 found similarly, concluding, "Although hundreds of millions of consumers and employees are obliged to use arbitration as their remedy, almost none do." Judith Resnik, Diffusing Disputes: The Public in the Private of Arbitration, the Private in Courts, and the Erasure of Rights, 124 Yale L.J. 2804 (2015).

[87] AAA, Consumer Mass Arbitration and Mediation Fee Schedule (amended and effective Jan. 15, 2024), https://www.adr.org/sites/default/files/Consumer_Mass_Arbitration_and_Mediation_Fee_Schedule.pdf; JAMS, Arbitration Schedule of Fees and Costs, https://www.jamsadr.com/arbitration-fees.

[88] J. Maria Glover, Mass Arbitration, 74 Stan. L. Rev. 1283, 1387, and Table 2 (2022).

[89] See, e.g., BuzzFeed Media Enters. Inc. v. Anderson, 2024 WL 2187054, at *1 (Del. Ch. May 15, 2024) (dismissing action to enjoin mass arbitration of claims brought by employees); Hoeg v. Samsung Elecs. Am. Inc., No. 23-CV-1951 (N.D. Ill. Feb. 2024) (ordering defendant of BIPA claims brought by consumers to pay over $300,000 in AAA filing fees); Wallrich v. Samsung Elecs. Am. Inc., 2023 WL 5935024 (N.D. Ill. Sept. 12, 2023) (ordering defendant of BIPA claims brought by consumers to pay over $4 million in AAA fees); Uber Tech. Inc. v. AAA, 204 A.D.3d 506, 510 (N.Y. App. Div. 2022) (ordering defendant of reverse discrimination claims brought by customers to pay over $10 million in AAA case management fees).

[90] See, e.g., AAA Mass Arbitration Supplementary Rules (Jan. 15, 2024); JAMS Mass Arbitration Procedures and Guidelines (May 1, 2024).

[91] Wallrich v. Samsung Elecs. Am. Inc., 2024 WL 3249646, at *9 (7th Cir. July 1, 2024).

[92] Id.

[93] Id.

[94] Id.

[95] Id.

[96] See, e.g., Wikipedia, "IT Service Management," at https://en.wikipedia.org/wiki/IT_service_management, and "Service Catalog," at https://en.wikipedia.org/wiki/Service_catalog.

[97] See Thomas J. Parenty & Jack J. Donet, A Leader's Guide to Cybersecurity at 89, 118-26, 174-75, 180 (Harvard 2020) (discussing the security organization's responsibilities to maintain up-to-date inventories of computer systems on which critical business activities rely, and to systematically capture business changes).

[98] See, e.g., Wikipedia, "Enterprise Risk Management" (discussing typical risk functions in an ERM program), at https://en.wikipedia.org/wiki/Enterprise_risk_management.

[99] See, e.g., U.S. Dep't of Commerce, National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (Jan. 2023), at https://doi.org/10.6028/NIST.AI.100-1.