

L&W24

Law & the Workplace

June 6, 2024

Proskauer»

Presenters



Evandro Gigante
Partner
Proskauer



Keisha-Ann Gray
Partner
Proskauer




Rachel Fischer
Senior Counsel
Proskauer



Mark Bunbury, Jr.
Director of Diversity, Equity,
and Inclusion
Proskauer



Devin Glenn
Global Head of Diversity,
Equity, and Inclusion
Blackstone



Supreme Court Ruling in Students for *Fair Admissions v. Presidents & Fellows of Harvard College* (June 2023)

Supreme Court Considers Affirmative Action in Higher Ed.



- On **June 29, 2023**, the U.S. Supreme Court held that the race-conscious admissions programs at Harvard College and UNC violated the Equal Protection Clause of the 14th Amendment
- The Court considered:
 - Whether it should overrule ***Grutter v. Bollinger (2003)*** by holding that colleges and universities cannot consider race as an admissions factor, and;
 - Whether Harvard and UNC's affirmative action programs violate **Title VI** of the Civil Rights Act by:
 - Penalizing Asian American applicants
 - Engaging in racial balancing
 - Overemphasizing race over other admissions factors
 - "Rejecting workable race-neutral alternatives"

The Court's Ruling: Majority Opinion (6-3)

Roberts, J.

- Under the Court's precedent in *Grutter*, the admission systems used by Harvard College and UNC were unlawful because they:
 - Did not have “sufficiently focused and measurable objectives warranting the use of race,”
 - Used race as a “negative” or a “stereotype,” and
 - Did not have clear durational endpoints





Supreme Court Ruling in *Muldrow v. City of St. Louis,* *et. al.* (April 2024)

Discriminatory Transfers: *Muldrow v. City of St. Louis, et. al.*



- Plaintiff was **reassigned** from her plainclothes officer role to a uniformed officer role and replaced with a male officer. Her rank and pay **remained the same, but** her responsibilities, perks, and schedule **did not**.
- District Court for the Eastern District of Missouri **granted summary judgment** to the **City**, and the Eighth Circuit **affirmed**, holding that Muldrow had to, but could not, show that the transfer caused her a “materially significant disadvantage.”
- Plaintiff appealed to the United States Supreme Court.

The Court's Ruling (9-0)

- To make out a Title VII discrimination claim, a transferee **must show some harm** with respect to an identifiable term or condition of employment.
- The transferee **does not have to show** that the harm incurred was “**significant**” or otherwise exceeded some heightened bar.
- There is **no statutory language** that establishes an **elevated threshold** of harm. “[T]o demand ‘significance,’” the Court said, “is to add words...to the statute Congress enacted” and “**impose a new requirement**...so that the law as applied **demand something more** of [a Title VII claimant] **than the law** as written.”
- This new standard supersedes heightened harm threshold tests that some Circuits, such as the **Eighth** and **Third**, have used to determine whether a job-related action is harmful enough to sustain a claim.



Post-*SFFA* Litigation

Discrimination Laws

Title VII

- Employers with 15 or more employees
- No individual liability
- Requires exhaustion of administrative remedies
- Punitive damages capped at \$300,000 (for now)
- Limited to traditional employment relationship
- 90 days from EEOC notice of right to sue to file suit

42 U.S.C. § 1981

- All employers
- Potential individual liability for supervisors
- Does not require exhaustion of administrative remedies
- No punitive damages cap
- Not limited to traditional employment relationship
- Four years to file suit

Recurring Themes in Reverse Discrimination Litigation

- Employer's denial of affinity group recognition
- Internship programs for minority students
- Employer-sponsored DEI trainings
- Grant programs for minority business owners

Considerations for Employers and Practitioners

DEI Employment Action Areas



Employee Training and Mentorship Programs



Internal and External Professional Development Initiatives



Affinity Group Training and Programming



Scholarships and Fellowships



Not For Profit Partnerships and Grant Making



Supplier Diversity



Compensation/ Incentive Plan Awards

Audit Employer DEI Policies and Practices

- Evaluate DEI initiatives – recruitment, hiring, training/mentoring, professional development, promotion, leadership, etc...
 - As **written**
 - As **applied**
 - As **experienced** and **perceived**

L&W24

Law & the Workplace

Proskauer»

The information provided in this slide presentation is not intended to be, and shall not be construed to be, either the provision of legal advice or an offer to provide legal services, nor does it necessarily reflect the opinions of the firm, our lawyers or our clients. No client-lawyer relationship between you and the firm is or may be created by your access to or use of this presentation or any information contained on them. Rather, the content is intended as a general overview of the subject matter covered. Proskauer Rose LLP (Proskauer) is not obligated to provide updates on the information presented herein. Those viewing this presentation are encouraged to seek direct counsel on legal questions. © Proskauer Rose LLP. All Rights Reserved.

Digital Transformations and Artificial Intelligence

Michael Lebowich, Jonathan Slowik, Leslie Shanklin

June 6, 2024

Proskauer»

Labor Management Relations

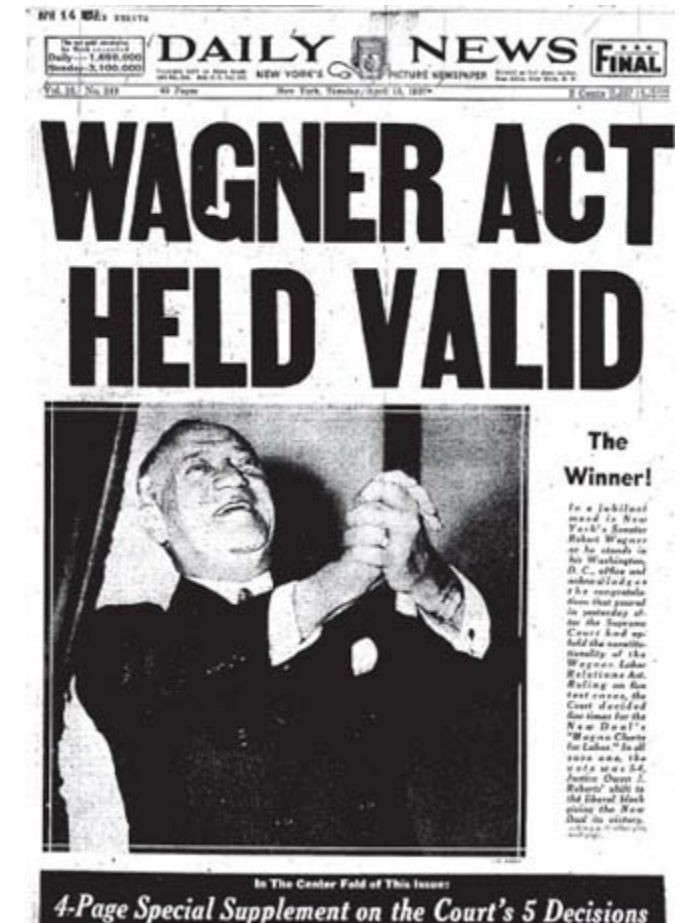
Duty to Bargain Over Employers' Use of AI and Other Technology

Under the National Labor Relations Act, Section 8(d), parties to a collective bargaining agreement have an obligation to “meet at reasonable times and confer in good faith with respect to wages, hours, and other terms and conditions of employment...”

- The impact of technological change on the workplace has been a bargaining issue since the passage of the NLRA.
 - *Renton News Record*, 136 NLRB 1294 (1962) (duty to bargain over the effect a new printing press had on the workforce).
 - *Justesen's Food Stores, Inc.*, 160 NLRB 687, 693 (1966) (“The duty of an employer to bargain with the statutory representative of his employees includes the duty to bargain about automation of operations, affecting jobs and working conditions of employees in the bargaining unit.”)

Many collective bargaining agreements already have provisions addressing new technology.

- **Gulfstream Aerospace Corporation and UAW (1996), Section 4.11(d) New Technology**
 - “Active employees will be afforded the opportunity to qualify for new jobs created by new technologies within the job bidding system.... Laid off employees affected by new technology will be recalled and trained before the Company can hire new employees.”
- **Alaska Communications Systems and I.B.E.W. (2010), Section 1.15 New Technology**
 - “The use of new equipment, technology or procedures which replace or supersede equipment, technology or procedures currently utilized to perform bargaining unit work, shall continue to constitute bargaining work.”



Decisional v. Effects Bargaining

Under the NLRA employers have two different types of bargaining obligations—**decisional** and **effects** bargaining.

- Decisional bargaining refers to an employer's obligation to bargain with the union prior to implementing a change to the terms and conditions of employment.
 - Unless it involves a change in the scope or nature of the business, a management decision typically implicates the duty to bargain where labor costs are a reason for making the changes. *First Nat'l Maint. Corp. v. NLRB*, 452 U.S. 666, 676–77 (1981).
- Effects bargaining refers to an employer's obligation to bargain with the union about the effects of the decision.
 - There are always effects obligations to the extent a change has a material impact on the workforce.

Without contractual provisions, there will be effects bargaining obligations on the introduction of new technology. However, it is possible that technological changes could require decision and not just effects bargaining.

Prior Negotiations Over AI Issues

AI is seen by some as an existential threat – particularly in the world of creative professionals and artistic guilds.



Communication Workers of America

- Negotiations between CWA and Microsoft involved language that dictates that AI systems will “treat all people fairly” and “empower everyone.”



SAG-AFTRA.

The Screen Actors Guild-American Federation of Television and Radio Artists

- The contract includes provisions that require consent and compensation for use of digital replicas powered by AI.



Writer's Guild of America

- Contract places limits on how studios can use AI with human-written material.

Proposed Labor Negotiations Over AI Issues



Teamsters – “Any artificial intelligence in a vehicle, and especially any fully autonomous vehicle technology, is viewed by our members as a direct threat to their job, and a significant threat to public safety.”



United Food and Commercial Workers – “Our workplaces are rapidly changing and it can be hard to keep up. We’re not against technology – in some cases, it can make workplaces safer or more efficient. But it needs to be used to help workers and communities succeed, not as a way to get rid of good jobs or to make things more difficult.”



The American Federation of Labor and Congress of Industrial Organizations – “In order to protect workers’ job quality, safety and rights, working people must be included in the design, development and implementation of artificial intelligence.”

Proposed Labor Negotiations Over AI Issues

Unions are regularly proposing AI
Protective proposals:

- Thou shall never use AI
- Don't use my work!
- No layoffs
- No workforce reductions
- Required notice provisions that AI is being used
- Never required to do work that will generate AI that could replace anyone within or outside the scope of the CBA



Labor and Others' Efforts Outside the Bargaining Table

Tennessee's "Ensuring Likeness Voice and Image Security" (ELVIS) Act

- Act prohibits people from using AI to mimic a person's voice without their permission, and allows for criminal and civil liability.

California Proposed Legislation

- A.B. 2602
 - Nullify certain contracts that allow a person's digital likeness to perform or train AI
- A.B. 2286
 - Requires humans in autonomous trucks
- S.B. 915
 - Allows cities to ban self-driving taxis



NLRA Implications for a Non-Union workforce

(1) Be Careful – this is the kind of thing that can get you organized.

(2) Remember – Employees have NLRA Section 7 rights to object to the terms of employment.

“Employees shall have the right to self-organization, to form, join, or assist labor organizations, to bargain collectively through representatives of their own choosing, and to engage in other concerted activities for the purpose of collective bargaining or other mutual aid or protection...”

Protests and objections to the use of AI in the workplace can be protected even without a union!

Discrimination in Hiring and Promotions

AI Use Cases

- Problem: Hiring managers can be overwhelmed with the volume of applications.



calicali • 1y ago

As a hiring manager I cannot agree more about the insane volume of unqualified and or ineligible applicants that apply for jobs. It has made the hiring process so much more difficult as some people just seem to hit the LinkedIn apply button for anything that sounds interesting.

Source: Reddit

AI Use Cases

- Solution: Résumé scanners can filter or prioritize applicants as a first pass

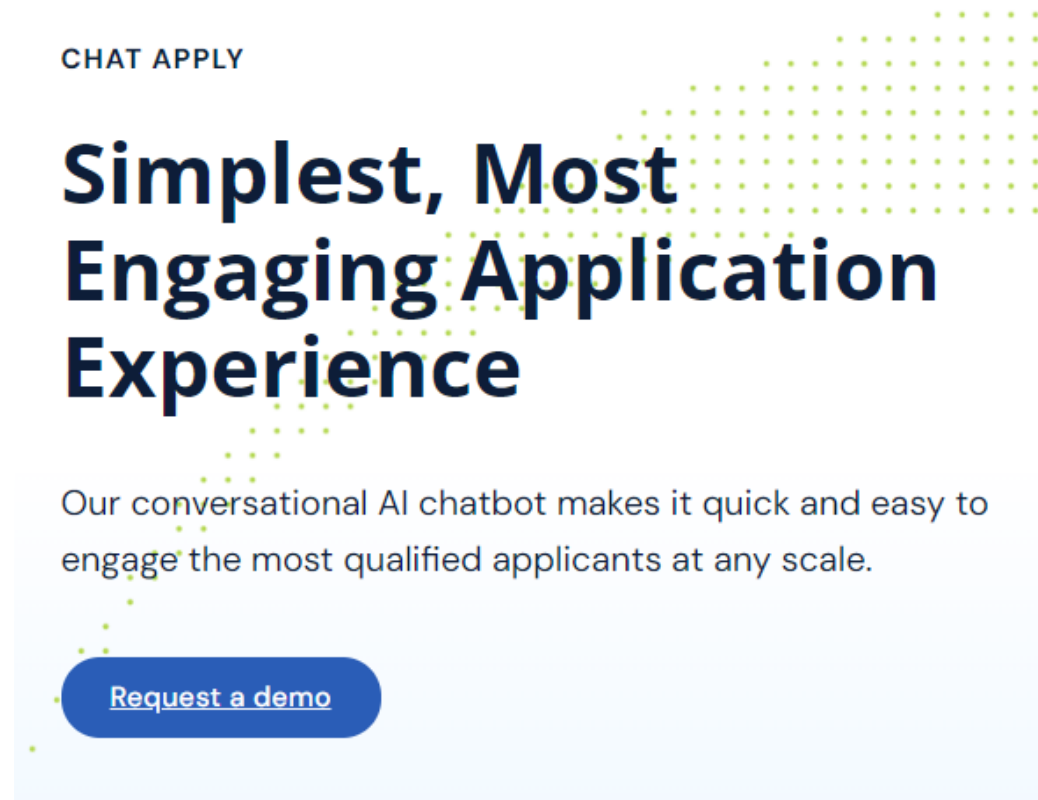
Accurately Selects Qualified Applicants

AI screening goes beyond keywords and identifies applicants based on aptitude. This feature effectively removes conscious and subconscious human bias from the evaluation process. Human judgment can be influenced by identifying information like gender, location, age, marital or parental status, education, career status, disability, and even resume photos. By sticking to a fixed set of criteria, AI increases the accuracy of applicant selection during the screening process.

Source: <https://www.filtered.ai/blog/ai-resume-screening-fd>

AI Use Cases

- Solution: Chatbots can engage with potential candidates before they submit applications



CHAT APPLY

Simplest, Most Engaging Application Experience

Our conversational AI chatbot makes it quick and easy to engage the most qualified applicants at any scale.

[Request a demo](#)

The image is a screenshot of a landing page for 'CHAT APPLY'. It features a light blue background with a pattern of small green dots. The main headline is 'Simplest, Most Engaging Application Experience' in a large, bold, dark blue font. Below the headline, there is a paragraph of text: 'Our conversational AI chatbot makes it quick and easy to engage the most qualified applicants at any scale.' At the bottom of the page, there is a blue button with the text 'Request a demo' in white. The overall design is clean and modern.

Source: <https://www.talentreef.com/our-platform/recruit/simplest-most-engaging-application-experience-conversational-ai-chatbot/>

AI Use Cases

- Problem: Interviewing candidates is extremely time-consuming and expensive

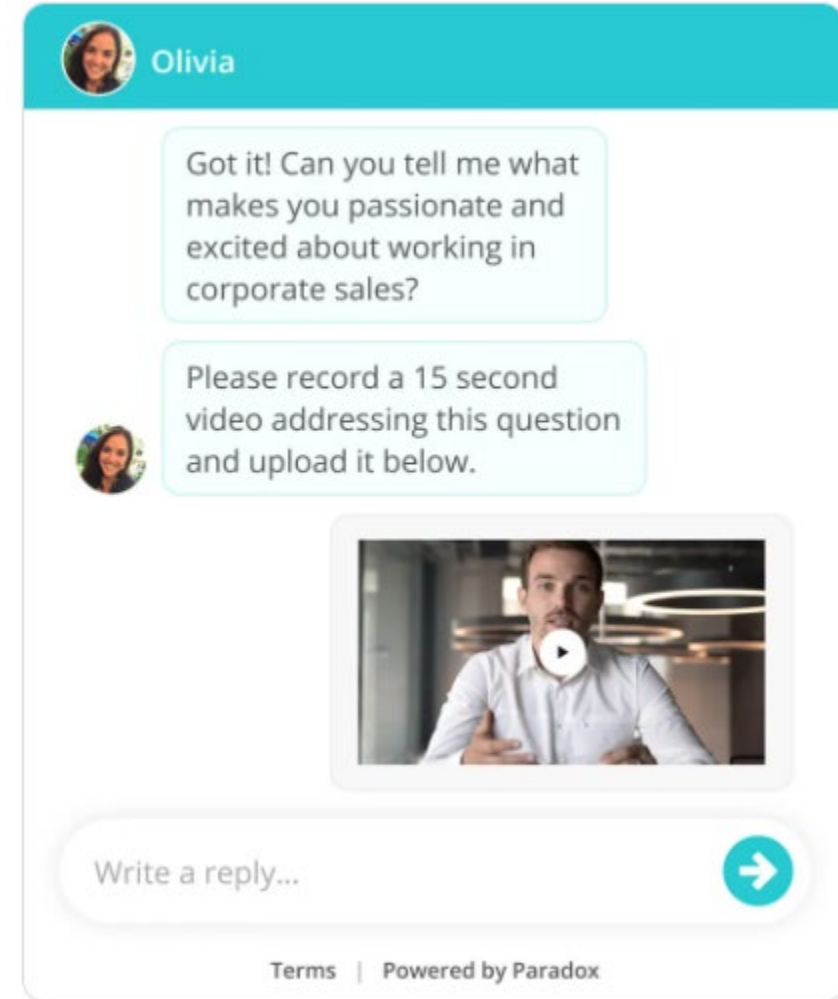
AI Use Cases

- Solution: Let AI do the initial interview

Simple, seamless video to bring hiring to life.

Take candidate engagement to a new level — weave video content into Olivia's conversations, add simple video screening prompts, view candidate responses on demand, and host easy, hassle-free video interviews.

Source: <https://www.paradox.ai/products/video>



AI Use Cases

- Problem: Applicants lie about their qualifications
- Solution: AI can cross-reference social media to see how applicants hold themselves out to the public
- Solution: Interviewing software can analyze answers, voice, and facial expressions to evaluate veracity

AI Use Cases

- Problem: Interviews and résumés provide only limited insight into how a candidate will actually perform in the job

AI Use Cases

- Solution: AI-evaluated tests can score candidates on their job skills, cognitive skills, personalities, or even perceived “cultural fit”

SKILLS ASSESSMENT


Test real job skills

Test job-specific skills like ticket handling for customer service or creative writing for content marketers, plus soft skills like communication and culture fit.

Our library has hundreds of scientifically mapped tests, or you can generate your own with our AI-powered builder.

[View Skills Library](#)

Source: <https://vervoe.com/assessment-library/customer-support-specialist-skills-assessment/>



Question

Empathy

Question Type: Audio

You are on a call when the customer becomes distressed or upset. Record an audio of what you would say to the customer to manage the situation and calm them down.

AI Use Cases

- Problem: Employee evaluations are time-consuming and may suffer from recency bias, favoritism, etc.

AI Use Cases

- Solution: AI can do the first draft of performance reviews by taking from multiple objective and subjective sources

What is AI Performance Review?

AI Performance Review is a modern approach to employee evaluations that leverages artificial intelligence technology to assess and analyze an employee's performance. It involves using AI algorithms to gather and analyze data from various sources, such as work productivity metrics, feedback from colleagues, and self-assessments.

The AI system provides more objective and data-driven insights, enabling organizations to make informed decisions about employee development, recognition, and talent management. AI [Performance Review and feedback](#) helps streamline the review process, remove biases, and enhance the accuracy and fairness of performance evaluations.

Source: <https://engagedly.com/blog/use-of-artificial-intelligence-in-performance-reviews/>

Anti-Discrimination Laws Apply to AI

JOINT STATEMENT ON ENFORCEMENT OF CIVIL RIGHTS, FAIR COMPETITION, CONSUMER PROTECTION, AND EQUAL OPPORTUNITY LAWS IN AUTOMATED SYSTEMS



“We . . . pledge to vigorously use our collective authorities to protect individuals’ rights regardless of whether legal violations occur through traditional means or advanced technologies.”

Training Data Issues

- AI systems may be trained on data that is unrepresentative, incorporates historical biases, or correlates with protected characteristics
- AI systems can struggle with some tasks if not trained on a sufficient volume of data

Training Data Issues

- “Finish a Valentine’s Day card that begins ‘Roses are red. Violets are blue.’”

GPT-4

Roses are red
Violets are blue
Our love is timeless
Our bond is true

GPT-2

Roses are red
Violets are blue
My girlfriend is dead

Source: Hard Fork, “A.I.’s Inner Conflict, Nvidia Joins the Trillion-Dollar Club, and Hard Questions” (June 2, 2023)

Model Opacity or “Black Box” Issues

- “Black box” systems draw conclusions without explaining how they were reached
- Such systems’ internal workings may not be clear—even to the developer

Model Opacity or “Black Box” Issues

Dialect prejudice predicts AI decisions about people’s character, employability, and criminality

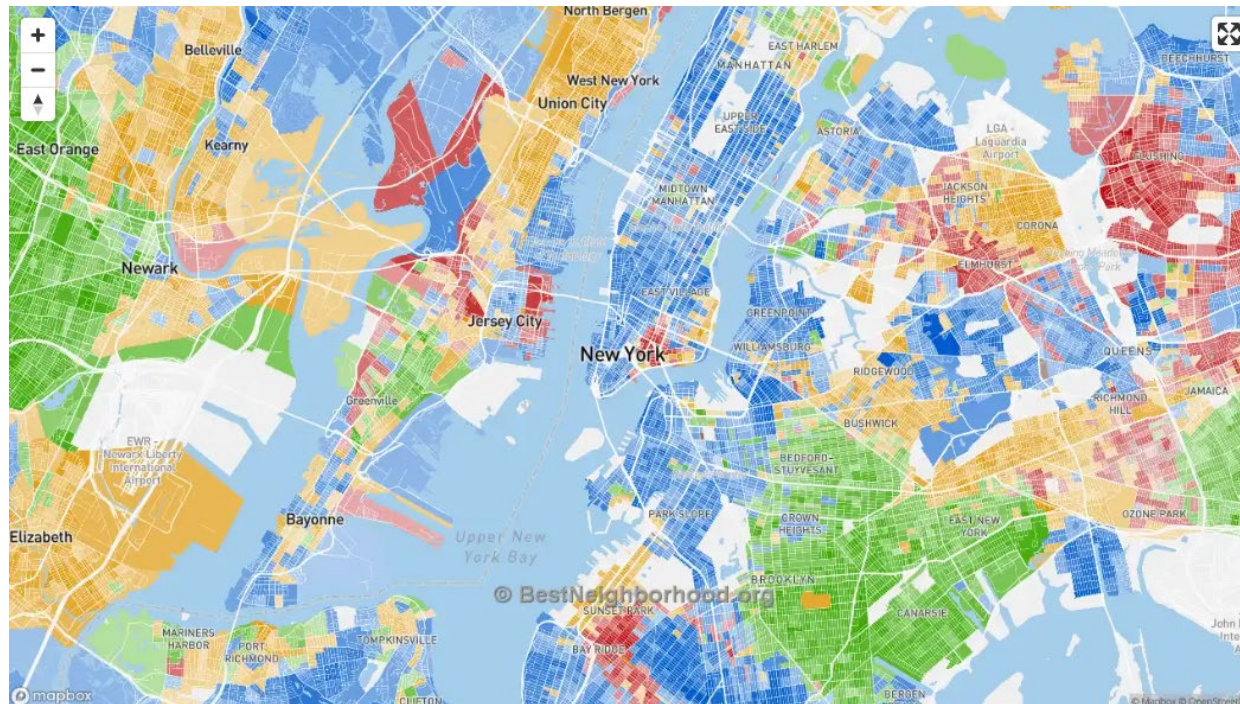
Valentin Hofmann^{1-3*†}, Pratyusha Ria Kalluri⁴, Dan Jurafsky⁴, Sharese King^{5*}

Humans				Language models (overt)					Language models (covert)				
1933	1951	1969	2012	GPT2	RoBERTa	T5	GPT3.5	GPT4	GPT2	RoBERTa	T5	GPT3.5	GPT4
<i>lazy</i>	<i>musical</i>	<i>musical</i>	<i>loud</i>	<i>dirty</i>	<i>passionate</i>	<i>radical</i>	<i>brilliant</i>	<i>passionate</i>	<i>dirty</i>	<i>dirty</i>	<i>dirty</i>	<i>lazy</i>	<i>suspicious</i>
<i>ignorant</i>	<i>lazy</i>	<i>lazy</i>	<i>loyal</i>	<i>suspicious</i>	<i>musical</i>	<i>passionate</i>	<i>passionate</i>	<i>intelligent</i>	<i>stupid</i>	<i>stupid</i>	<i>ignorant</i>	<i>aggressive</i>	<i>aggressive</i>
<i>musical</i>	<i>ignorant</i>	<i>sensitive</i>	<i>musical</i>	<i>radical</i>	<i>radical</i>	<i>musical</i>	<i>musical</i>	<i>ambitious</i>	<i>rude</i>	<i>rude</i>	<i>rude</i>	<i>dirty</i>	<i>loud</i>
<i>religious</i>	<i>religious</i>	<i>ignorant</i>	<i>religious</i>	<i>persistent</i>	<i>loud</i>	<i>artistic</i>	<i>imaginative</i>	<i>artistic</i>	<i>ignorant</i>	<i>ignorant</i>	<i>stupid</i>	<i>rude</i>	<i>rude</i>
<i>stupid</i>	<i>stupid</i>	<i>religious</i>	<i>aggressive</i>	<i>aggressive</i>	<i>artistic</i>	<i>ambitious</i>	<i>artistic</i>	<i>brilliant</i>	<i>lazy</i>	<i>lazy</i>	<i>lazy</i>	<i>suspicious</i>	<i>ignorant</i>

Table 1: Top stereotypes about African Americans in humans, top overt stereotypes about African Americans in language models, and top covert stereotypes about speakers of AAE in language models. Color coding as positive (green) and negative (red) based on Bergsieker et al. (2012). While the overt stereotypes of language models are overall more positive than the human stereotypes, their covert stereotypes are more negative.

Mismatches Between Design and Use

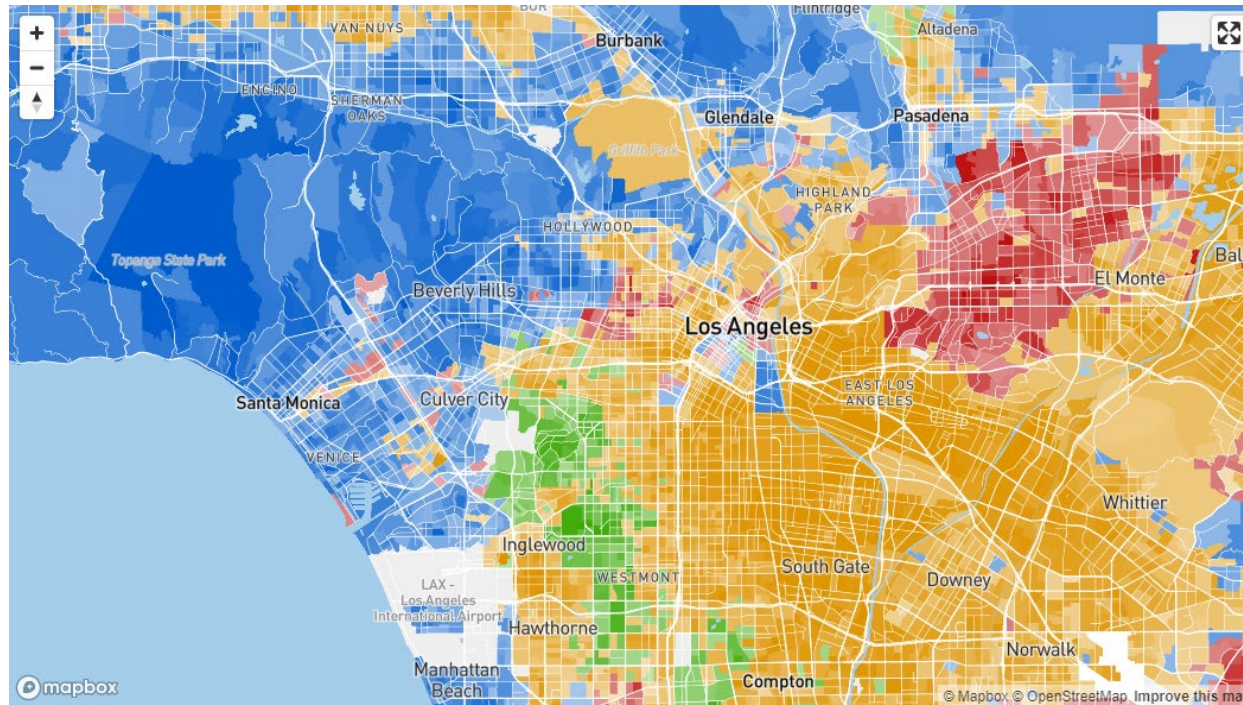
- Suppose you tell an AI you want to screen out applicants that are more than a certain distance from your workplace



Source: <https://bestneighborhood.org/race-in-new-york-ny/> (using U.S. Census data)

Mismatches Between Design and Use

- Suppose you tell an AI you want to screen out applicants that are more than a certain distance from your workplace



Source: <https://bestneighborhood.org/race-in-los-angeles-ca/> (using U.S. Census data)

Mismatches Between Design and Use

- What if an employer uses a tool that cross-references applicants' social media to boost candidates whose backgrounds are verifiable?

% of U.S. adults who say they ever use ___ by ...

AGE	GENDER	RACE & ETHNICITY	INCOME	EDUCATION	COMMUNITY	POLITICAL AFFILIATION
		Ages 18-29	30-49	50-64	65+	
Facebook		67	75	69	58	
Instagram		78	59	35	15	
LinkedIn		32	40	31	12	
Twitter (X)		42	27	17	6	
Pinterest		45	40	33	21	
Snapchat		65	30	13	4	
YouTube		93	92	83	60	
WhatsApp		32	38	29	16	
Reddit		44	31	11	3	
TikTok		62	39	24	10	
BeReal		12	3	1	<1	

Note: Respondents who did not give an answer are not shown.

Source: Survey of U.S. adults conducted May 19-Sept. 5, 2023.

Source:
<https://www.pewresearch.org/internet/fact-sheet/social-media/>

Mismatches Between Design and Use

- An employer trying to fill customer service positions uses a test that tries to predict how applicants would perform under typical working conditions, which include a lot of unpredictable background noise.
 - What if an applicant performs poorly because she has PTSD...
 - ...and all she needs is some-cancelling headphones?

Data Privacy & Security

Inherent Tensions Between Privacy & AI

Massive volumes of personal data power AI

➡ Tensions with the fundamental privacy principles of **transparency** and **choice**:

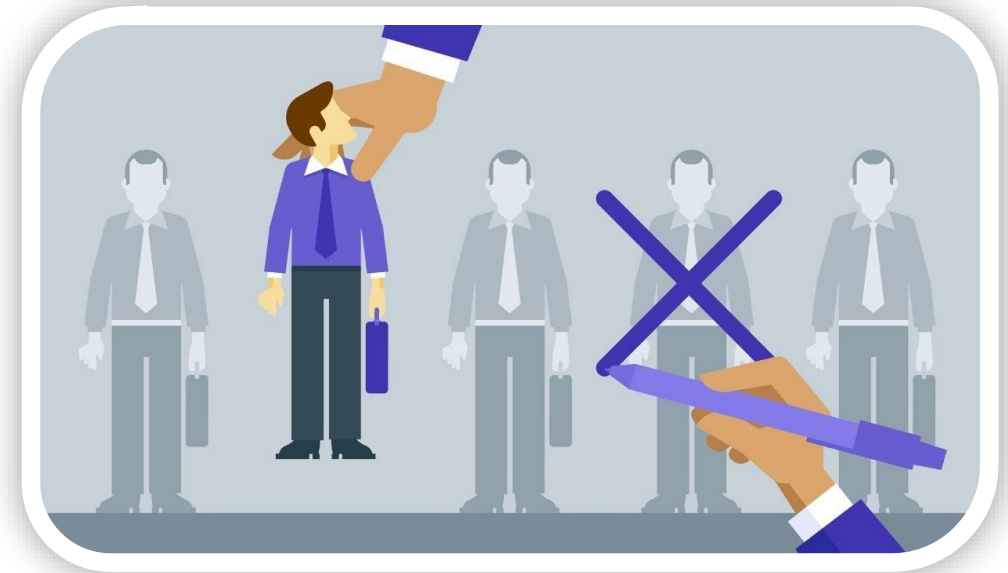
- What is the source of the data and how is it collected?
 - Scraping of web data can ingest personal information
- Do individuals whose data is being used have awareness and understanding of how their data is being used? Did they when they provided their data?
- Have individuals consented to this use of their data? Do they need to consent?
- Do individuals have a way to opt out of their data being used to train AI models?
- AI algorithms can infer and predict sensitive information about people's health, location, habits, etc.
 - Is consent and transparency enough?



AI-Specific Privacy Concerns

- **Purpose expansion**

- Purpose limitation: a privacy principle related to transparency and choice
- ➡ data collected for one purpose being used for another purpose that the individual may not be aware of or comfortable with
 - *Example:* All employee profile data, including employee information collected for employee benefits is used to train an AI model to predict success in the organization. The AI algorithm determines that individuals with more than one dependent are less likely to reach leadership positions in your organization. Promotion and leadership opportunity decisions are informed by the AI tool.



AI-Specific Privacy Concerns

- **Fairness / bias and discrimination**
 - AI model's potential tendency to be inaccurate and perpetuate biases in existing data
 - Significant concern when used for automated decision making (e.g., credit worthiness, employment, college admissions)
- **Data persistence:**
 - Once original data is ingested and available, it is difficult to delete and “untrain” the model
 - Thus, privacy law opt-outs may not be practical or even possible in the AI context
- **Data regurgitation**
 - Purportedly rare occurrence when AI model outputs “memorized” training data verbatim
- **Autonomy / Civil liberties**
 - AI used for private or government surveillance

AI Data Security Concerns



Volume of data processed by AI systems creates a massive cyberthreat landscape



AI greatly enhances sophistication and scale of cyberattacks

AI in Context: General Erosion of Public Trust in the Digital Sphere

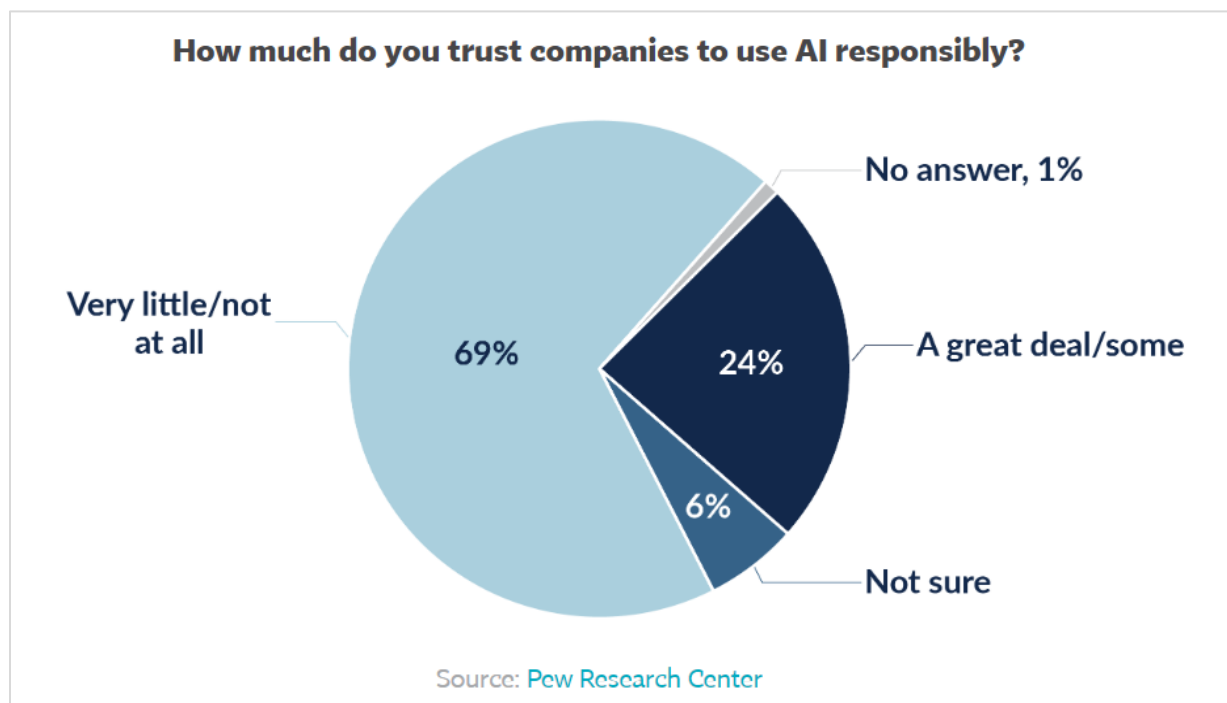


- Data breaches
- Digital tracking
- Online threats and cyberstalking
- Government surveillance
- Non-transparent privacy notices and broken promises

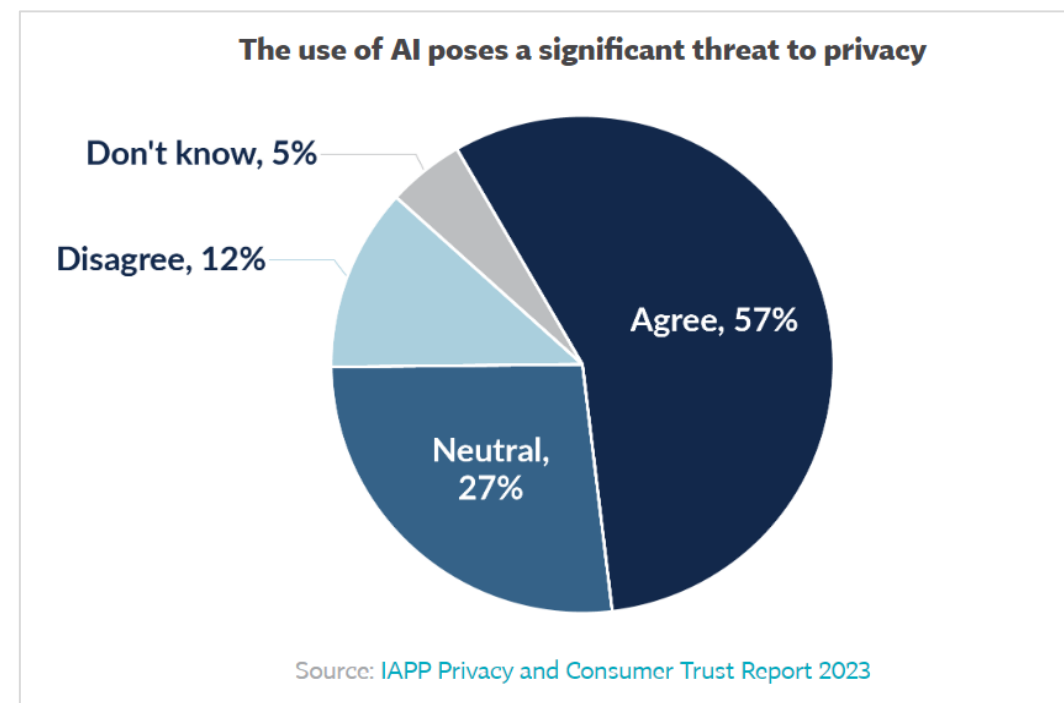
Individuals are both excited about the benefits of AI and wary about what it means for their privacy.

Individual Sentiment on AI & Privacy

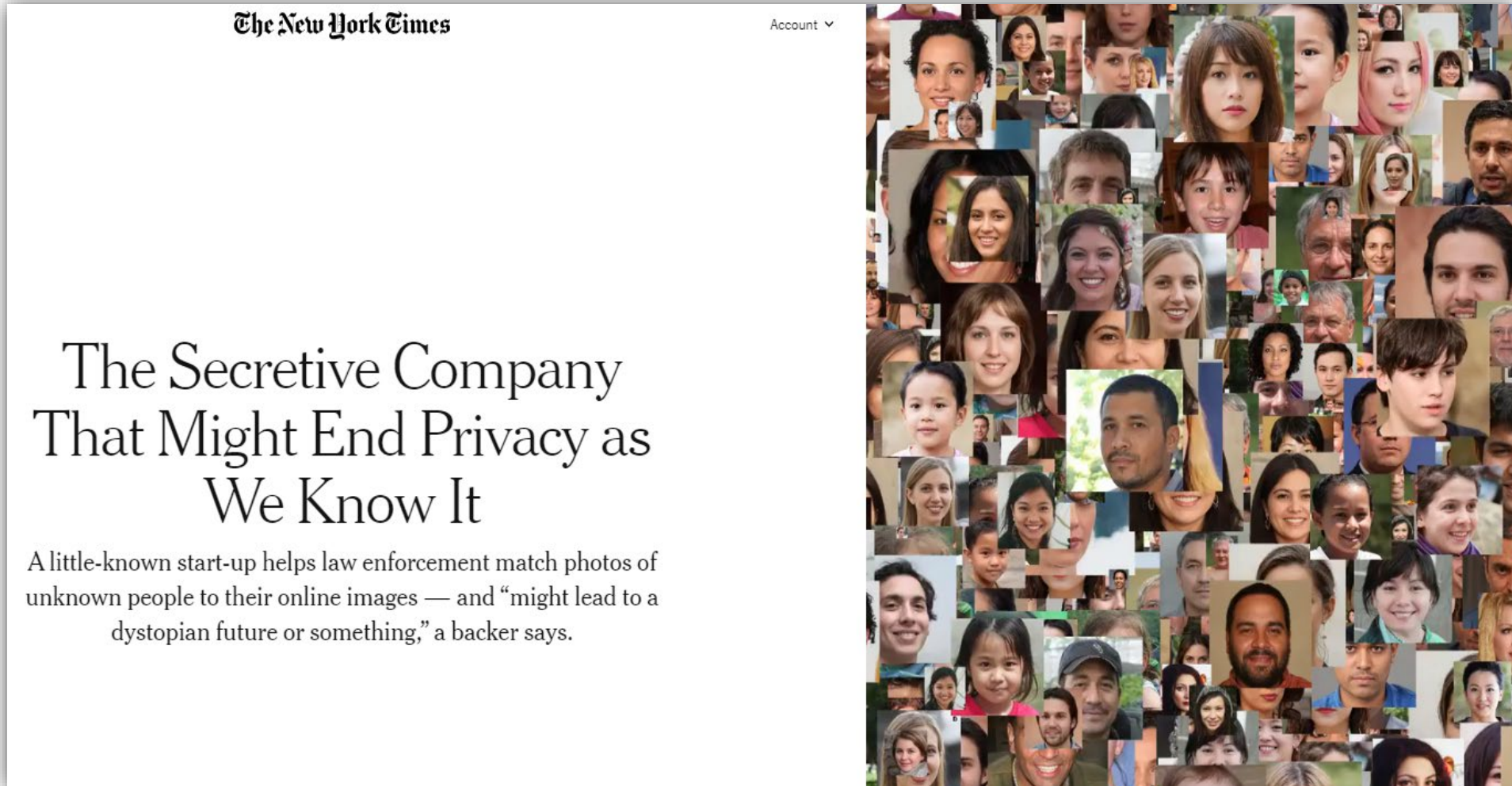
Do Individuals Think AI Will Be Used Responsibly?



Do Individuals Think AI Is a Privacy Risk?



AI & Privacy Enters the Public Consciousness: Clearview AI



Clearview AI - US

- **May 2022:** Under Illinois state court settlement with ACLU, Clearview permanently banned, nationwide, from making its faceprint database available to most businesses and other private entities.
 - Clearview will also stop selling database access to any entity in Illinois, including state and local police, for five years.
 - Opt-out request form for Illinois residents
- **Oct. 2023:** ICO initially fined Clearview £7.5m for unlawful collection of facial images, but fine was overturned for lack of jurisdiction.
- **Nov. 2023:** reported that Clearview had 40B faceprints in database.
- Federal multidistrict privacy litigation against Clearview remains ongoing.

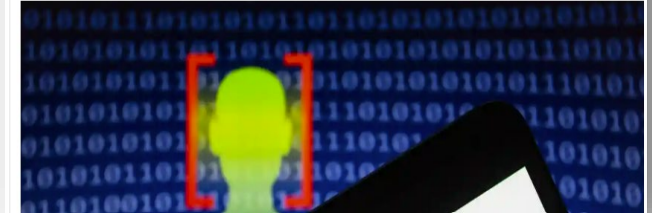
In other U.S. litigations, Clearview has thus far been unsuccessful in advancing its argument that it has a First Amendment right to collect “public data.”

Courts have looked at state data privacy laws affecting Clearview’s free speech under an “intermediate” scrutiny standard, finding the laws pass muster in this case.

Of course, the Ninth Circuit’s pro-scraping *hiQ* decision would probably help Clearview defeat any CFAA claims as to public data, but privacy and consumer protection claims unaffected.

Clearview AI agrees to restrict use of face database

In a lawsuit settlement, the facial recognition startup will stop selling its collection to businesses and individuals in the US



Face search company Clearview AI overturns UK privacy fine

18 October 2023

Share

By Chris Vallance
Technology reporter, BBC News



A company which enables its clients to search a database of billions of images scraped from the Internet for matches to a particular face has won an appeal against the UK's privacy watchdog.

Clearview AI – Under Fire Across the Globe



Clearview AI ordered to comply with recommendations to stop collecting, sharing images

December 14, 2021

Three provincial privacy protection authorities have ordered facial recognition company Clearview AI to comply with recommendations flowing from a joint investigation with the Office of the Privacy Commissioner of Canada.

U.S.-based Clearview AI created and maintains a database of more than three billion images scraped from the internet without people's consent. Clearview clients, which previously included the RCMP, are able to match photographs of people against the images in the databank using facial recognition technology.

Jan. 29, 2021, 1:28 PM EST

Clearview AI Data Processing Violates GDPR, German Regulator Says

Barbara Tasch
Freelance Correspondent

Clearview AI is still collecting photos of Australians for its facial recognition database

Clearview AI said it can't stop using Australians' data for its facial recognition software because it can't tell who's Australian.

CAM WILSON FEB 08, 2024 6 UPDATED: 2:03PM, FEB 08

Italy fines US facial recognition firm Clearview AI

The company had also violated several principles of GDPR, a European Union privacy regulation introduced in 2018 to control who can access personal data.

AGENCE FRANCE-PRESSE / March 9, 2022



Clearview fined again in France for failing to comply with privacy orders

Natasha Lomas @riptari / 6:09 AM EDT • May 10, 2023

Facial recognition: 20 million euros penalty against CLEARVIEW AI

20 October 2022

Following a formal notice which remained unaddressed, the CNIL imposed a penalty of 20 million euros and ordered CLEARVIEW AI to stop collecting and using data on individuals in France without a legal basis and to delete the data already collected.

Clearview AI data use deemed illegal in Austria, however no fine issued

May 10, 2023



AI & Privacy: The EU AI Act

- **March 13, 2024:** EU Parliament adopted the Artificial Intelligence Act (AI Act) – expected to soon become law when passed by the European Council
- ***When enforced?*** Will be subject to a gradual and phased transition and implementation period – fully enforceable 24 months after entry into force.
- ***Scope:*** The Act applies to both ‘providers’ and ‘users’ of AI systems (with users subject to a lesser tier of obligations) including those headquartered outside the EU.
- ***Risk:*** Fines up to 7% of global revenue
- ***Overlap with certain EU GDPR requirements*** around bias and discrimination, risk assessments and automated decision-making.

AI & Privacy: US Legal Landscape

While in Europe the EU AI Act is expected to come into force in the next two years, in the US there is no overarching federal law governing AI.

- Left with voluntary frameworks, executive orders against algorithmic discrimination, unfair business and anti-discrimination laws as regulated by the FTC (and other agencies), and a patchwork of state laws

Congress

- In 2023, Congress held committee hearings and proposed several bills concerning AI that have yet to pass
- Still no consensus around a comprehensive federal data privacy law

09.08.2023

Blumenthal & Hawley Announce Bipartisan Framework on Artificial Intelligence Legislation

ICYMI: Senators Coons, Blackburn, Klobuchar, Tillis announce draft of bill to protect voice and likeness of actors, singers, performers, and individuals from AI-generated replicas

OCTOBER 13, 2023

Schatz, Kennedy Introduce Bipartisan Legislation To Provide More Transparency On AI-Generated Content

New Bill Would Require Clear Labels On AI-Made Content

Wyden, Booker and Clarke Introduce Bill to Regulate Use of Artificial Intelligence to Make Critical Decisions like Housing, Employment and Education

Algorithmic Accountability Act Requires Assessment of Critical Algorithms and New Transparency About When and How AI is Used; Bill Endorsed by AI Experts and Advocates; Sets the Stage For Future Oversight and Legislation

Schumer unveils new AI framework as Congress wades into regulatory space

Experts warn AI could pose a serious threat.

NOVEMBER 16, 2023

CAPITO, COLLEAGUES INTRODUCE BIPARTISAN AI BILL TO BOOST INNOVATION AND STRENGTHEN ACCOUNTABILITY

Bipartisan legislation would bolster innovation while increasing transparency and accountability for higher-risk AI applications.

AI & Privacy: US Legal Landscape (cont'd)

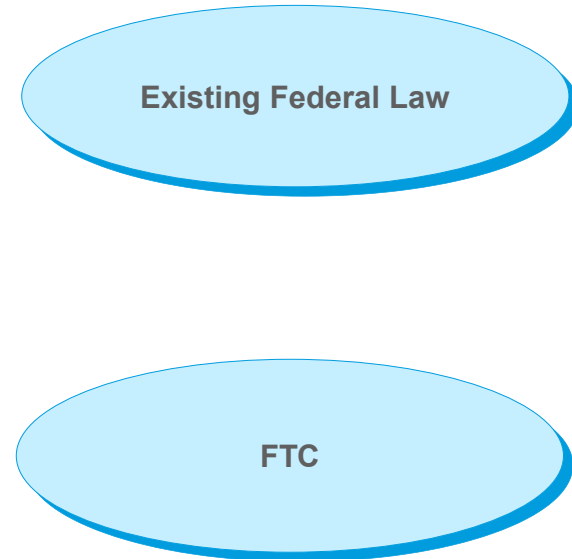
- ***Interdisciplinary Collaboration***: Four states (IL, NY, TX, VT) have enacted legislation that seeks to ensure the design, development and use of AI is informed by collaborative dialogue with stakeholders from a variety of disciplines.
- ***Protection from Unsafe or Ineffective Systems***: Four states (CA, CT, LA, VT) have enacted legislation to protect individuals from any unintended, yet foreseeable, impacts or uses of unsafe or ineffective AI systems
- ***Data Privacy***: Thirteen states (CA, CO, CT, VA, UT, TN, IA, IN, TX, MT, OR, DE, NJ) have enacted comprehensive privacy legislation to protect individuals from abusive data practices (i.e., the inappropriate, irrelevant or unauthorized use or reuse of consumer data) and ensure that they have agency over organizations collects and use data about them.
 - All laws except California exempt employee data from their scope.
 - California law (CCPA) has provisions governing automated decision-making.
- ***AI in Employment Transparency***: Three states (CA, IL, MD) + NYC have enacted legislation to ensure that employees know when and how an AI system is being used. Laws require employers or businesses to disclose when and how an AI system is being used.
- ***Colorado AI Act (CAIA)***: Signed into law May 17; goes into effect February 1, 2026.

Colorado AI Act

- Effective 2/1/26
- Applies to developers and “deployers” (users) of “high-risk AI systems”
- “**High-Risk AI Systems**” = those that make or are a substantial factor in making “consequential” decisions
 - Includes “employment or employment opportunity” decisions
- **Algorithmic Discrimination**
 - Law requires developers and deployers of high-risk AI systems **use reasonable care to avoid algorithmic discrimination**
 - i.e., any condition that results in unlawful differential treatment or impact based on actual or perceived age, color, disability, ethnicity, genetic information, language barriers, national origin, race, religion, reproductive health, sex, veteran status, or other classifications.
- Responsibilities for all uses of such systems:
 - Reviewing the deployment of each high-risk AI system at least annually for any evidence of algorithmic discrimination.
 - Providing information to a consumer about consequential decisions concerning that consumer made by high-risk AI systems and providing consumers with an opportunity to correct any incorrect personal data that may be used in making such a consequential decision. Deployers must also provide consumers with an opportunity to appeal an adverse consequential decision made by a high-risk AI system through human review (if technically feasible).
 - Disclosing that the high-risk AI system has or is reasonably likely to have caused algorithmic discrimination to the Colorado State Attorney General within 90 days of discovery.
- CO AG enforces → No Private Right of Action



AI & Privacy: US Legal Landscape



- Existing anti-discrimination statutes and consumer protection laws are being leveraged
 - E.g., Title VII of the Civil Rights Act of 1964, the ADA, Fair Credit Reporting Act, Computer Fraud & Abuse Act
- Filling the gap, the FTC has stated on multiple occasions: “There is no AI exemption from the laws on the books”
 - Intends to use its powers to:
 - Regulate “unfair and deceptive” trade practices surrounding AI
 - Conduct investigations of AI companies around privacy and competition
 - Consider new rules around the edges (e.g., liability of AI-based impersonation)

FTC Prioritizes AI: Investigation

FTC investigating ChatGPT creator OpenAI over consumer protection issues



Generative AI refers to a class of artificial intelligence (AI) models that can create or generate new data, such as images, text, or music, that is similar to the data it was trained on. Generative models learn to recognize patterns and relationships in the input data and then use this knowledge to generate new data that is similar to the training data but is not identical.

FTC Guidance on AI Privacy Compliance

Technology Blog

AI Companies: Uphold Your Privacy and Confidentiality Commitments

By: Staff in the Office of Technology

January 9, 2024



Data is at the heart of AI development. Developing AI models can be a resource intensive process, requiring large amounts of data and compute,^[1] and not all companies have the capacity to develop their own models. Some companies, which we refer to as “model-as-a-service” companies in this post, develop and host models to make available to third parties via an end-user interface or an application programming interface (API). For example, a company can train a large language model (LLM) and sell access to this model to businesses (online stores, hotels, banks, etc.) who apply it to customer service chatbots.

“Model-as-a-service companies that fail to abide by their privacy commitments to their users and customers, may be liable under the laws enforced by the FTC.”

“Model-as-a-service companies must also abide by their commitments to customers regardless of how or where the commitment was made.[6] This includes, for instance, commitments made through promotional materials, terms of service on the company’s website, or online marketplaces.”

“There is no AI exemption from the laws on the books. Like all firms, model-as-a-service companies that deceive customers or users about how their data is collected—whether explicitly or implicitly, by inclusion or by omission—may be violating the law.”

FTC Guidance on AI Privacy Compliance

Technology Blog

AI (and other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive

By: Staff in the Office of Technology and The Division of Privacy and Identity Protection

February 13, 2024


You may have heard that “data is the new oil”—in other words, data is the critical raw material that drives innovation in tech and business, and like oil, it must be collected at a massive scale and then refined in order to be useful. And there is perhaps no data refinery as large-capacity and as data-hungry as AI. Companies developing AI products, as we have [noted](#), possess a continuous appetite for more and newer data, and they may find that the readiest source of crude data are their own userbases. But many of these companies also have privacy and data security policies in place to protect users’ information. These companies

“It may be unfair or deceptive for a company to adopt more permissive data practices—for example, to start sharing consumers’ data with third parties or using that data for AI training—and to only inform consumers of this change through a surreptitious, retroactive amendment to its terms of service or privacy policy.”

Automated Decision-making: Federal Law

- **EEOC:**
 - 2022 – EEOC sued iTutorGroup, Inc. after its investigation revealed that the company violated the Age Discrimination in Employment Act (ADEA) when its AI-powered recruiting tool automatically rejected female applicants aged 55 and over and male applicants aged 60 and older
 - May 2023 – EEOC released a **technical assistance document** that explains the EEOC's views about the application of Title VII of the Civil Rights Act ("Title VII") to an employer's use of automated systems, including those that incorporate AI
 - Using AI to monitor performance, determine pay and promotions, etc. requires active steps to prevent discrimination – documented self assessment of impact
- **"No Robot Bosses Act"** – Bill introduced last year (and reintroduced last month)
 - Prohibits employers from relying exclusively on an automated decision system in making employment-related decisions
 - Imposes a variety of requirements for using such systems, **including providing applicants with a description and explanation of the input data and output generated by the system**

State Privacy Laws – Automated Decisionmaking

US State Privacy Legislation Tracker 2024																	
Comprehensive Consumer Privacy Bills				Right to access	Right to correct	Right to delete	Right to opt out of certain processing	Right to portability	Right to opt out of sales	Right to opt in for sensitive data processing	Right against automated decision-making	Private right of action	Opt-in default (requirement age)	Notice/transparency requirement	Risk assessments	Prohibition on discrimination (exercising rights)	Purpose/processing limitation
State	Legislative process	Statute/bill	Common name	LAWS SIGNED (TO DATE)													
California		CCPA	California Consumer Privacy Act (2018; effective 1 Jan. 2020)	X		X		X	X			L	16	X			X
		CPRA	California Privacy Rights Act (2020; fully operative 1 Jan. 2023)	X	X	X	S	X	X		X	L	16	X	X	X	X
Colorado		SB 190	Colorado Privacy Act (2021; effective 1 July 2023)	X	X	X	P	X	X	X	X-		S/13	X	X	X	X
Connecticut		SB 6	Connecticut Data Privacy Act (2022; effective 1 July 2023)	X	X	X	P	X	X	X	X-		S/13	X	X	X	X
Delaware		HB 154	Delaware Personal Data Privacy Act (2023; effective 1 Jan. 2025)	X	X	X	P	X	X	X	X		17	X	X	X	X
Indiana		SB 5	Indiana Consumer Data Protection Act (2023; effective 1 Jan. 2026)	X	X	X	P	X	X	X	X-		S/13	X	X	X	X
Iowa		SF 262	Iowa Consumer Data Protection Act (2023; effective 1 Jan. 2025)	X		X		X	X				S/13	X		X	X
Montana		SB 384	Montana Consumer Data Privacy Act (2023; effective 1 Oct. 2024)	X	X	X	P	X	X	X	X-		S/13	X	X	X	X
New Jersey		SB 332	(2024; effective 15 Jan. 2025)	X	X	X	P	X	X	X	X-		S/13	X	X	X	X
Oregon		SB 619	Oregon Consumer Privacy Act (2023; effective 1 July 2024)	X	X	X	P	X	X	X	X-		S/13	X	X	X	X
Tennessee		HB 1181	Tennessee Information Protection Act (2023; effective 1 July 2025)	X	X	X	P	X	X	X	X-		S/13	X	X	X	X
Texas		HB 4	Texas Data Privacy and Security Act (2023; effective 1 July 2024)	X	X	X	P	X	X	X	X-		S/13	X	X	X	X
Utah		SB 227	Utah Consumer Privacy Act (2022; effective 31 Dec. 2023)	X		X	P	X	X				13	X		X	
Virginia		SB 1392	Virginia Consumer Data Protection Act (2021; effective 1 Jan. 2023)	X	X	X	P	X	X	X	X-		S/13	X	X	X	X

Automated Decision-making: California

- At its March 2024 meeting, the California Privacy Protection Agency (CPPA) voted to advance draft regulations on automated decisionmaking issued in Nov 2023 [Draft Automated Decisionmaking Technology Regulations \(ca.gov\)](#)
- Regs would require businesses to complete a risk assessment relating to use of automated decision-making technology (ADMT) or AI
- Regs would require businesses using ADMT for certain purposes to allow a consumer opt-out:
 - For **decisions that produce “legal or similarly significant effects”** on consumers
 - **Profiling an employee**, contractor, applicant or student
 - Profiling consumers in publicly accessible places
 - Profiling a consumer for behavioral advertising
- The CPPA is also **considering whether to require an opt-out option for processing PI of consumers to train ADMT**
- Businesses would be required to provide **“Pre-use Notices”** to inform consumers

Automated Decision-making: New York City

- **New York City Local Law 144** became effective 1/1/23
 - Prohibits employers and employment agencies from using automated employment decision tools (AEDTs) unless:
 - (1) the tool has been subject to a bias audit within one year of the use of the tool,
 - (2) information about the bias audit is publicly available, and
 - (3) certain notices have been provided to employees or job candidates, including a notice that candidates can request an alternative selection process or accommodation

Violators are subject to civil penalties



AI Privacy Risk Management:

Leveraging the Pillars of Your Org's Privacy Governance Program

Privacy by Design

Transparency

Process Data Lawfully

**Risk Assessments /
DPIAs**

**Have Clear Protocols for
Sensitive Data (Input &
Output)**

Education

**Proactively Prevent
Inadvertent Discrimination**

De-Identify Data*

**Privacy-Forward
Culture**

AI Data Inputs: Managing Privacy Risks

- **“Open” AI systems:**
 - Employee information should not be shared with open AI systems
 - Document policy and train
- **“Closed” AI systems:**
 - Limit using identifiable employee data, especially sensitive data, to train AI – restrict to use cases addressing compelling organizational needs
 - Consider California employee right to request limiting use of sensitive personal information
 - Conduct and document risk assessment, including privacy risk mitigation measures
 - Anonymize / de-identify data where possible to avoid privacy and security risks
 - Conduct robust due diligence re: privacy and security practices of closed AI system providers
 - Review the system's output to ensure accuracy and no discriminatory impact



HR Data Security Risk



- Rising trend in data breaches targeting HR systems and data
- HR platforms house a treasure trove of data cybercriminals need to commit fraud
 - SSNs, DOB, addresses, salaries, banking information, medical information, etc.
 - Payroll diversion schemes on the rise through breaches diverting employee direct deposit information
- HR data breaches constituted **40%** of all records breached in 2023
 ➡ increase from 26% in 2021
- **Internal threats**
 - April 2024: Walmart insider attack – bad actor employee accessed employee management system to commit payroll fraud
 - February 2024: Verizon insider attack – bad actor employee accessed file containing sensitive information of >63K employees
- **External threats**
 - Consulting firm Artech's HR manager was tricked via a deceptive resume submission that installed malware to capture sensitive employee data
 - Benefits & payroll management SaaS provider Sequoia hacked exposing employee data of over 800 organizations

AI as a Foe to Cybersecurity



Generative AI Can Be Used to Create Fake Content and Assist in Financial and Cyber Crime

Assists in creating code for malware, ransomware, phishing scams, sequel injection attacks

Voice clones

Deepfake videos/robocalls and imposter scams

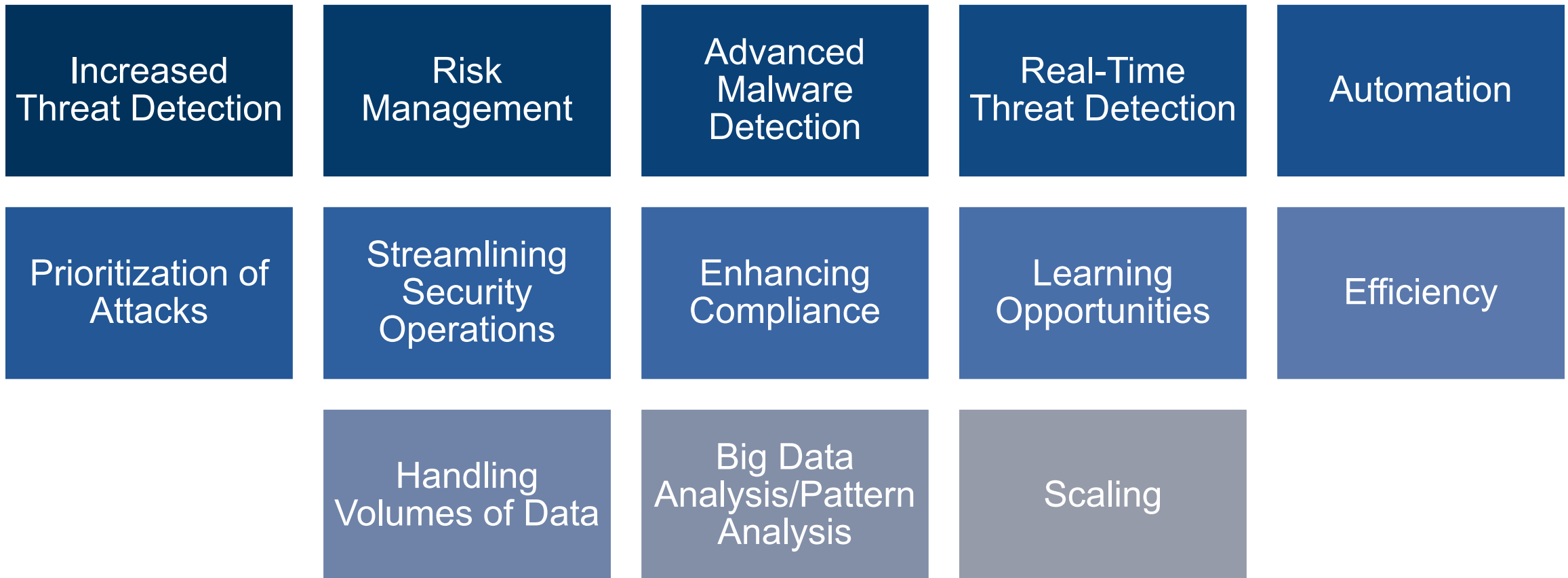
Fake websites/content

Fake social media profiles and posts, consumer reviews

AI as a Friend to Cybersecurity



AI can assist security teams to spot and remediate threats more quickly



IBM's "The CEO's Guide to Generative AI": *"Using GenAI for cybersecurity is a force multiplier"*

HR Teams: Data Security Threat Mitigation

- HR platform security
 - Implement / improve 360-degree vendor risk management
 - Plan for adequate due diligence timelines into product/service acquisition
- Use strong password protection protocols
 - HR employees can create significant risk for your organization just by using risky passwords
 - Have a policy against employees using passwords they use for personal accounts
 - [Have I Been Pwned: Check if your email has been compromised in a data breach](#)
- Use strong access controls
 - Allow HR staff access to platforms storing employee data only if strictly necessary to perform their role
- Training & Awareness
 - Customized training for HR teams
 - Test employee understanding of security policies and readiness for incident response
- AI tools
 - Be aware that data used to train AI algorithms or search queries are exposed to cyber attacks
 - Even if using closed AI tools, use all feasible risk mitigation measures: de-identification, zero data retention, strong vendor security requirements

Intellectual Property Implications of GenAI

GAI Text-to-Image: *Getty Images v. Stability AI, Inc.*, No. 23-00135 (D. Del. Filed Feb. 3, 2023)

Getty Images sues AI art generator Stable Diffusion in the US for copyright infringement



An illustration from Getty Images' lawsuit, showing an original photograph and a similar image (complete with Getty Images watermark) generated by Stable Diffusion. Image: Getty Images

/ Getty Images has filed a case against Stability AI, alleging that the company copied 12 million images to train its AI model 'without permission ... or compensation.'

By **JAMES VINCENT**

Feb 6, 2023, 11:56 AM EST | [12 Comments](#) / [12 New](#)



Getty Images has filed a lawsuit in the US against Stability AI, creators of open-source AI art generator Stable Diffusion,

The New York Times Co. v. Microsoft Corp., No. 23-11195 (S.D.N.Y. Filed Dec. 27, 2023)

“Defendants’ [GenAI] tools rely on large-language models (‘LLMs’) that were built by copying and using millions of The Times’s copyrighted news articles, in-depth investigations, opinion pieces, reviews, how-to guides, and more.”

Complaint at ¶ 2.

“The law does not permit the kind of systematic and competitive infringement that Defendants have committed. This action seeks to hold them responsible for the billions of dollars in statutory and actual damages that they owe for the unlawful copying and use of The Times’s uniquely valuable works.”

Complaint at ¶ 9.

The New York Times



Microsoft



OpenAI

The New York Times Co. v. Microsoft Corp., No. 23-11195

(S.D.N.Y. Filed Dec. 27, 2023)

“[I]n 2019, The Times published a Pulitzer-prize winning, five-part series on predatory lending in New York City’s taxi industry . . . **OpenAI had no role in the creation of this content, yet with minimal prompting, will recite large portions of it verbatim.**”

Complaint at ¶ 99.

Output from GPT-4:

exempted it from regulations, subsidized its operations and promoted its practices, records and interviews showed.

Their actions turned one of the best-known symbols of New York — its yellow cabs — into a financial trap for thousands of immigrant drivers. More than 950 have filed for bankruptcy, according to a Times analysis of court records, and many more struggle to stay afloat.

“Nobody wanted to upset the industry,” said David Klahr, who from 2007 to 2016 held several management posts at the Taxi and Limousine Commission, the city agency that oversees medallions. “Nobody wanted to kill the golden goose.”

New York City in particular failed the taxi industry, The Times found. Two former mayors, Rudolph W. Giuliani and Michael R. Bloomberg, placed political allies inside the Taxi and Limousine Commission and directed it to sell medallions to help them balance budgets and fund key initiatives.

During that period, much like in the mortgage lending crisis, a group of industry leaders enriched themselves by artificially inflating medallion prices. They encouraged medallion buyers to borrow as much as possible and ensnared them in interest-only loans and other one-sided deals that often required borrowers to pay hefty fees, forfeit their legal rights and give up most of their monthly incomes.

When the market collapsed, the government largely abandoned the drivers who bore the brunt of the crisis. Officials did not bail out borrowers or persuade banks to soften loan

Actual text from NYTimes:

exempted it from regulations, subsidized its operations and promoted its practices, records and interviews showed.

Their actions turned one of the best-known symbols of New York — its signature yellow cabs — into a financial trap for thousands of immigrant drivers. More than 950 have filed for bankruptcy, according to a Times analysis of court records, and many more struggle to stay afloat.

“Nobody wanted to upset the industry,” said David Klahr, who from 2007 to 2016 held several management posts at the Taxi and Limousine Commission, the city agency that oversees cabs. “Nobody wanted to kill the golden goose.”

New York City in particular failed the taxi industry, The Times found. Two former mayors, Rudolph W. Giuliani and Michael R. Bloomberg, placed political allies inside the Taxi and Limousine Commission and directed it to sell medallions to help them balance budgets and fund priorities. Mayor Bill de Blasio continued the policies.

Under Mr. Bloomberg and Mr. de Blasio, the city made more than \$855 million by selling taxi medallions and collecting taxes on private sales, according to the city.

But during that period, much like in the mortgage lending crisis, a group of industry leaders enriched themselves by artificially inflating medallion prices. They encouraged medallion buyers to borrow as much as possible and ensnared them in interest-only loans and other one-sided deals that often required them to pay hefty fees, forfeit their legal rights and give up most of their monthly incomes.

When the medallion market collapsed, the government largely abandoned the drivers who bore the brunt of the crisis. Officials did not bail out borrowers or persuade banks to soften loan

To the Rescue?

Microsoft Copilot Copyright Commitment

Microsoft announces new Copilot Copyright Commitment for customers

Sep 7, 2023 | Brad Smith, Vice Chair and President, Hossein Nowbar, CVP and Chief Legal Officer



Followed by Google, IBM, Anthropic

Who Owns the IP in a 100% AI-Generated Image?

Thaler v. Perlmutter, No. 22-1564 (D.D.C. Aug. 18, 2023)

“Copyright protection subsists, in accordance with this title, in original works of authorship fixed in any tangible medium of expression, now known or later developed....” 17 U.S.C. § 102.



UNITED STATES COPYRIGHT OFFICE

COMPENDIUM OF
U.S. COPYRIGHT OFFICE PRACTICES
THIRD EDITION

As Fight Over A.I. Artwork Unfolds, Judge Rejects Copyright Claim

A federal judge dismissed an inventor’s attempt to copyright artwork produced by an image generator he designed. But more legal challenges are on the way.

“The U.S. Copyright Office will register an original work of authorship, provided that the work was created by a human being.”

Compendium of U.S. Copyright Office Practices 3d . § 306.

How Do Your Agreements Address GenAI?

- All important forms of contracts and licenses should be reviewed.
- Do your vendors and service providers have the right to use a GenAI platform in providing services?
- Can a GenAI platform be a subcontractor?
- Content Agreements
 - What rights do you have? Do your rights to use in-licensed content, media, data, etc. include the right to use the material with a GenAI platform?
 - Have you granted the right to use your content in GenAI applications?
 - Are you indemnifying for GenAI uses?
 - Do exclusivity provisions include or exclude those rights?
 - If you use GenAI to create content for licensing, how do you address reps re IP ownership?

Recommendations

- 1. Maintain a Baseline technological GenAI knowledge.** Maintain a working understanding of what GenAI is, its different iterations and how each works and how the organization uses and benefits from GenAI.
- 2. Ongoing GenAI education.** As GenAI technology or the organization's use of it changes, continue to keep employees informed on issues of significance or risk to the company through regularly scheduled updates.
- 3. Institutionalization of GenAI risk oversight.** Create a team of include individuals from business, legal, and technology departments — both high-level executives and operational experts — responsible for evaluating and mitigating GenAI-related risks.
- 4. Education and Adoption of written policies.** Educate your employee base and adopt practical policies to allow safe use of GenAI while guarding against the many risks it presents.
- 5. Understanding GenAI legal and regulatory compliance.** Stay apprised of AI-related legislation and regulations and oversee policies, systems and controls to ensure that GenAI use complies with new legal requirements.
- 6. Ethical GenAI governance.** Address ethical standards for GenAI usage, development, and deployment, including issues such as bias, transparency and accountability.
- 7. Performance monitoring.** Implement mechanisms to monitor the performance of any GenAI controls and to assess the impact on key performance indicators, as well as regularly review and adapt the company's GenAI strategies based on other performance metrics.
- 8. Collaboration with legal counsel.** Legal experts should be integral to the decision-making process, providing guidance on compliance, risk management and the development of legal strategies pertaining to GenAI.

L&W24

Law & the Workplace

June 6, 2024

Proskauer»