EBEC EXPO2024

Proskauer's Perspective on Employee Benefits, Executive Compensation and ERISA Litigation

Proskauer

Privacy, Data Security and AI: Ethics and Other Practice Pointers for Emerging Technology

Jeffrey D. Neuburger
Partner, Co-Chair, Technology, Media and Telecom
Leslie Shanklin
Partner, Chair, Privacy and Data Security

May 2, 2024

Proskauer

The General Release of ChatGPT on November 30, 2022

Introducing ChatGPT

Nov 30, 2022

Proskauer

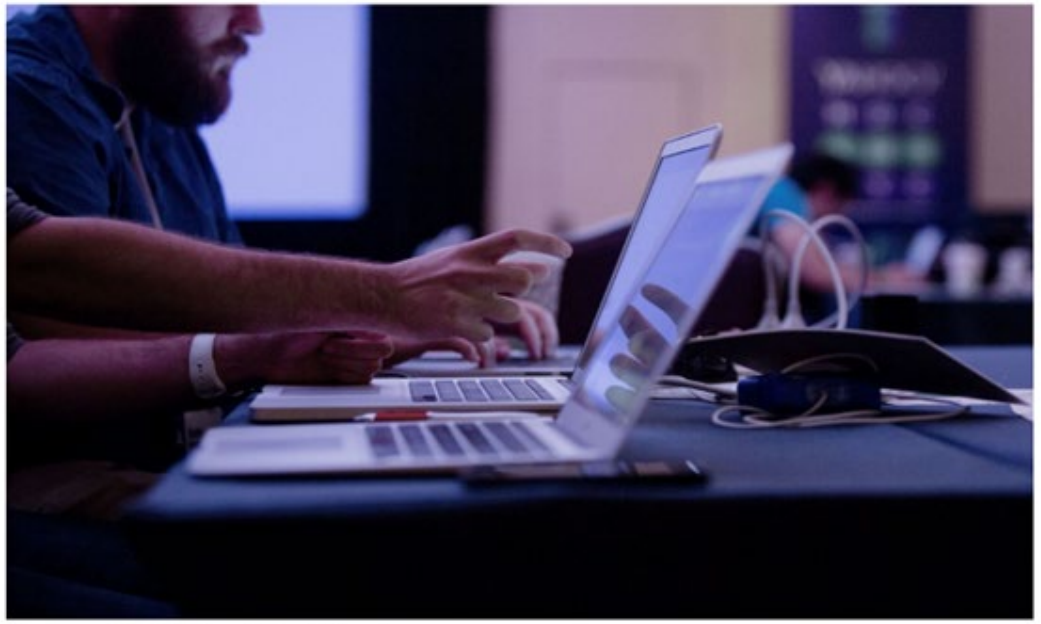
Everything Changed on January 3, 2023

Bloomberg

● Live Now Markets Economics Industries Tech AI Politics Wealth Pursuits Opinion Businessweek

Newsletter
Technology & Skills

Work Shift: Ringing in 2023 With ChatGPT



Photographer: Victor J. Blue/Bloomberg

By Jo Constantz

January 3, 2023 at 10:45 AM EST

Proskauer

Generative AI and the EBEC Practices

Proskauer

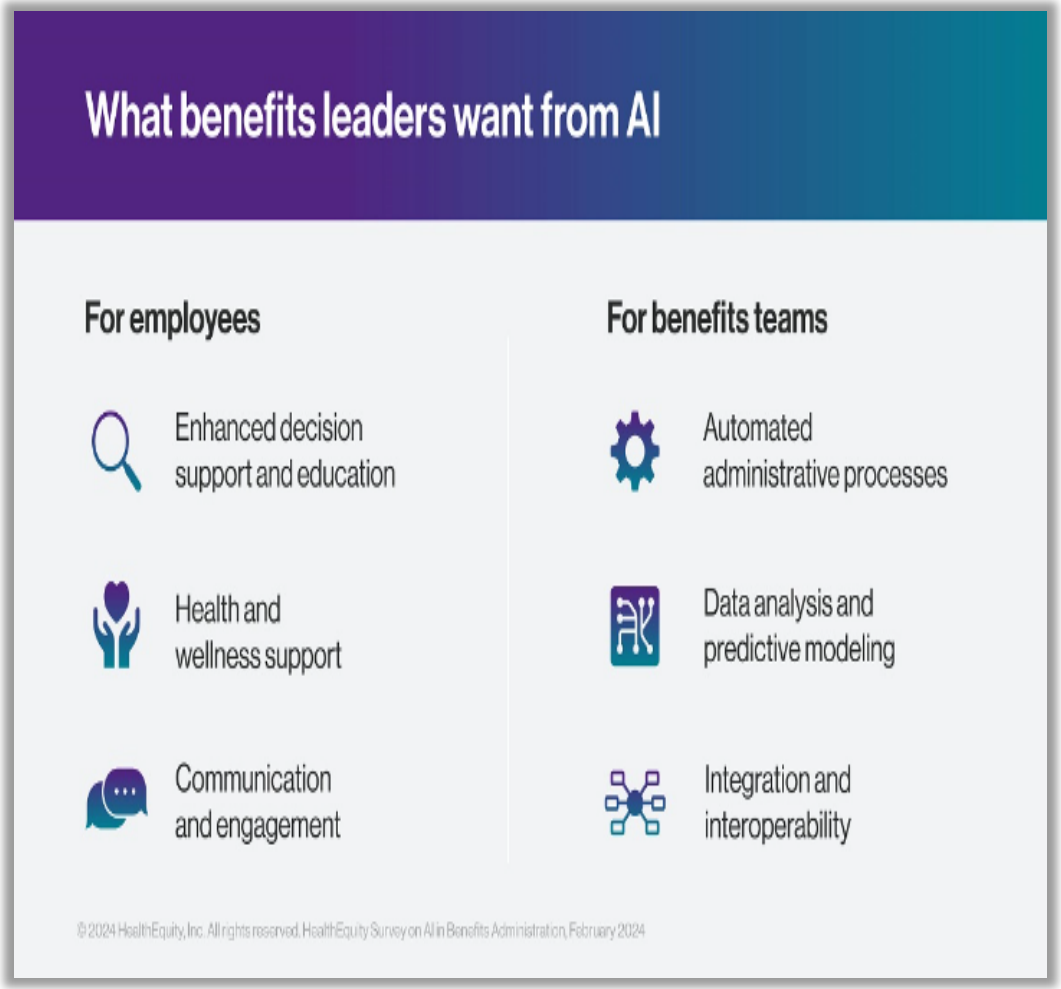
A Note on Industry Use

HR Insights

HealthEquity

Survey: Top benefits leaders see opportunities and concerns in AI

March 27, 2024 • 5 min read



Proskauer

A Note on Industry Use – Robo Advisors

DEPARTMENT OF LABOR

Employee Benefits Security Administration

29 CFR Part 2510

RIN 1210–AC02

Retirement Security Rule: Definition of an Investment Advice Fiduciary

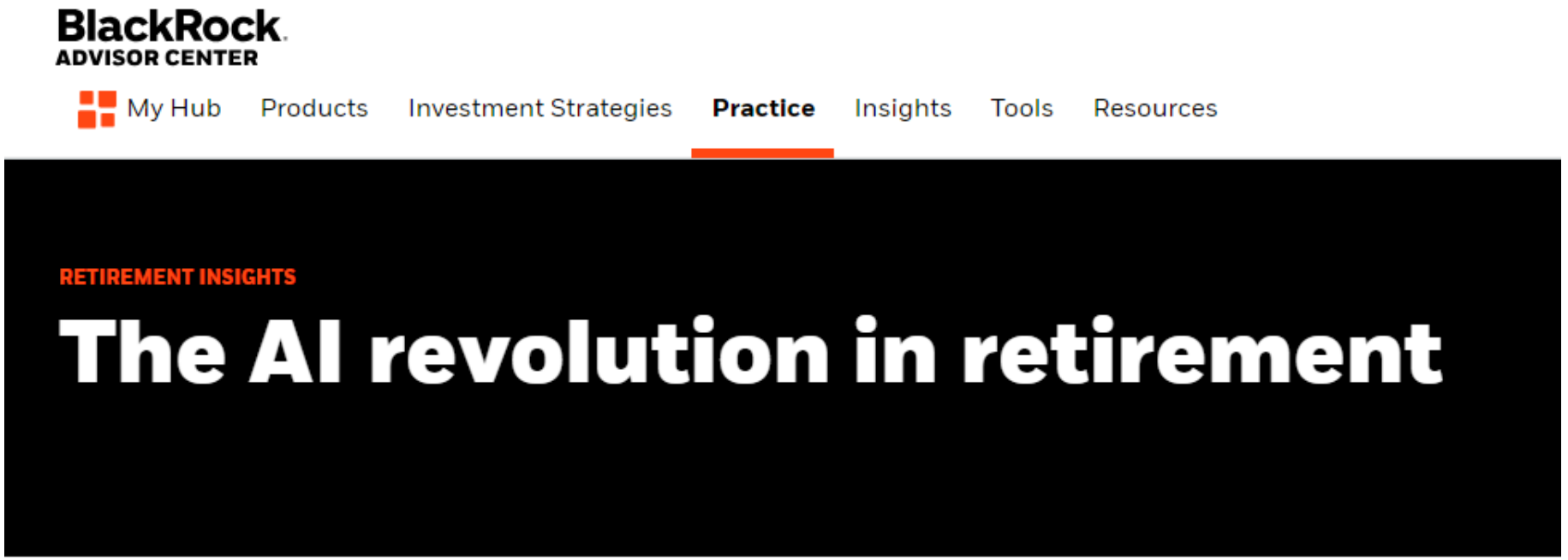
AGENCY: Employee Benefits Security Administration, Department of Labor

ACTION: Final rule

SUMMARY: The Department of Labor (Department) is adopting a final rule defining when a person renders "investment advice for a fee or other compensation, direct or indirect" with respect to any moneys or other property of an employee benefit plan, for purposes of the definition of a "fiduciary" in the Employee Retirement Income Security Act of 1974 (Title I of ERISA or the Act). The final rule also applies for purposes of Title II of ERISA to the definition of a fiduciary of a plan defined in Internal Revenue Code (Code), including an individual retirement account or other plan identified in the Code..

- How will robo-advisors meet fiduciary duty requirements under ERISA?
- How can fiduciaries evaluate and monitor robo-advisor performance?
- How will AI fee analyses comply with a sponsor's legal obligations to pay reasonable fees and expenses?

A Note on Industry Use



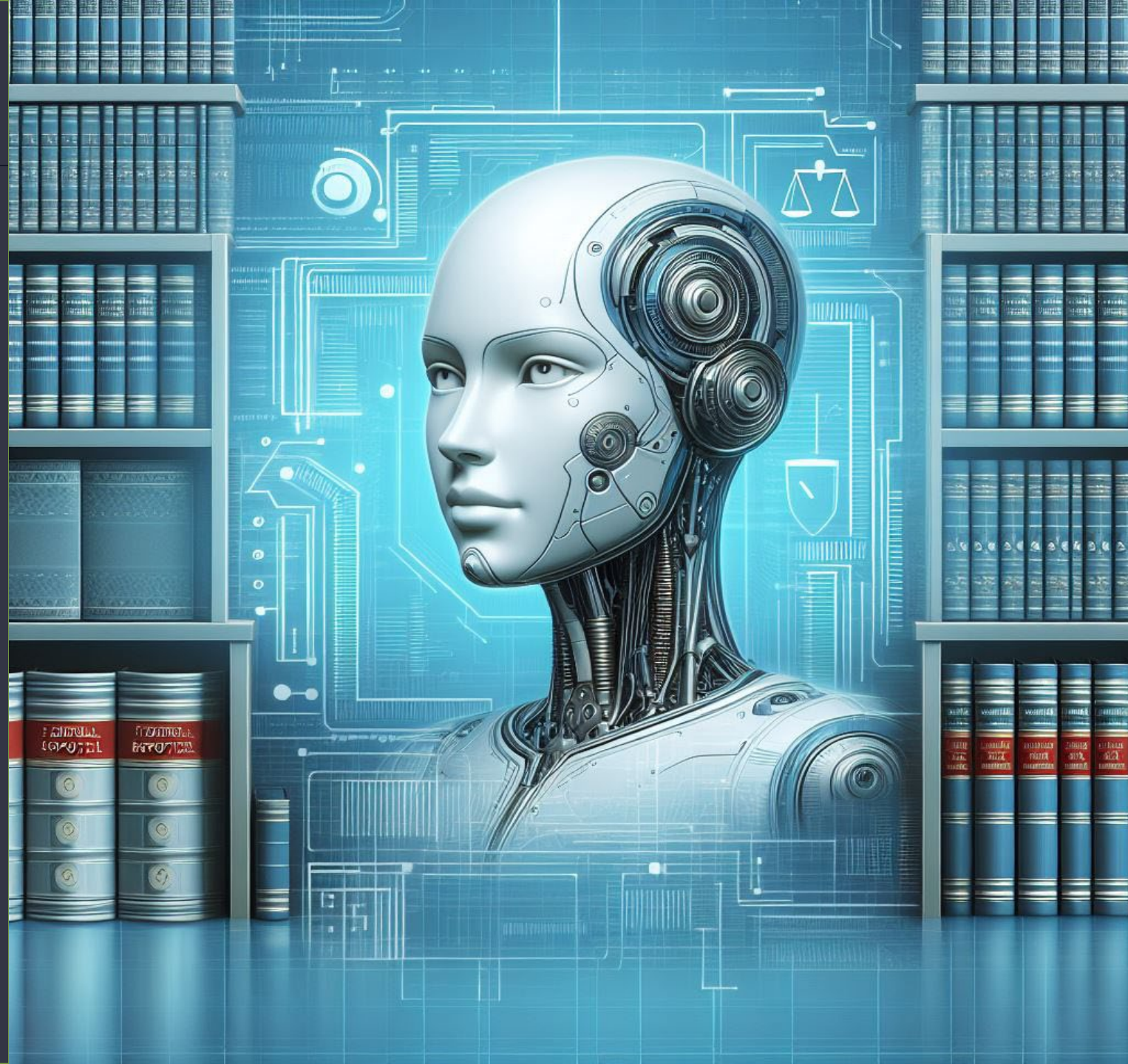
Proskauer

Duty of Competence

A lawyer shall provide **competent representation** to a client. Competent representation requires the legal knowledge, skill, thoroughness, and preparation reasonably necessary for the representation.

- *ABA Model Rule 1.1*

—ABA Model Rule 1.1

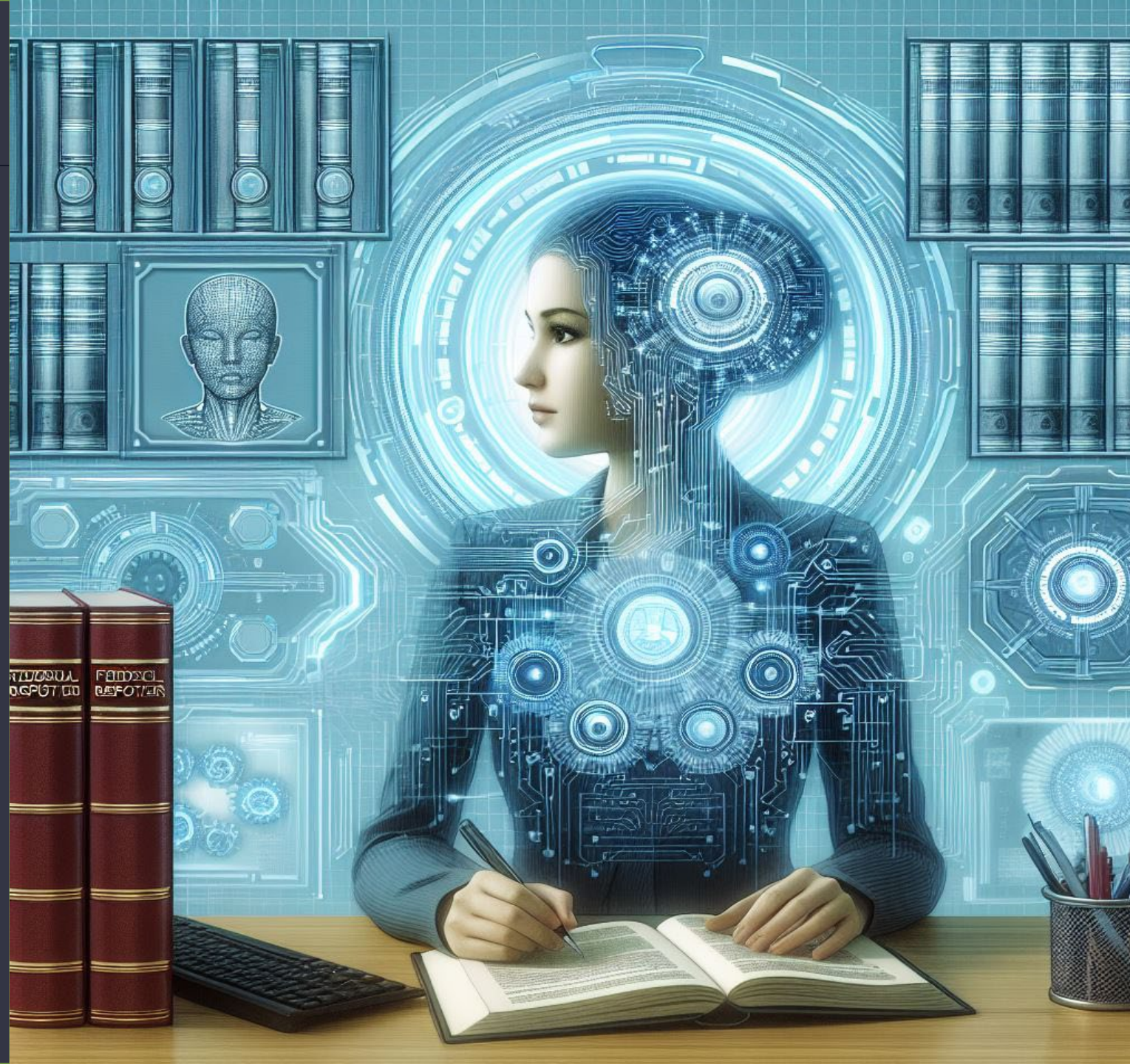


Duty of Competence

Comment 8 to Model Rule 1.1 : "To maintain the requisite knowledge and skill, **a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology,** engage in continuing study and education and comply with all continuing legal education requirements to which the lawyer is subject."

—Comment 8 to AB

NYSBA Comm. on Prof'l Ethics, Op. 1025 (2014): "**An attorney should only use technology that he or she is competent to use.**"*A Model Rule 1.1*



How does a Generative AI System Work?

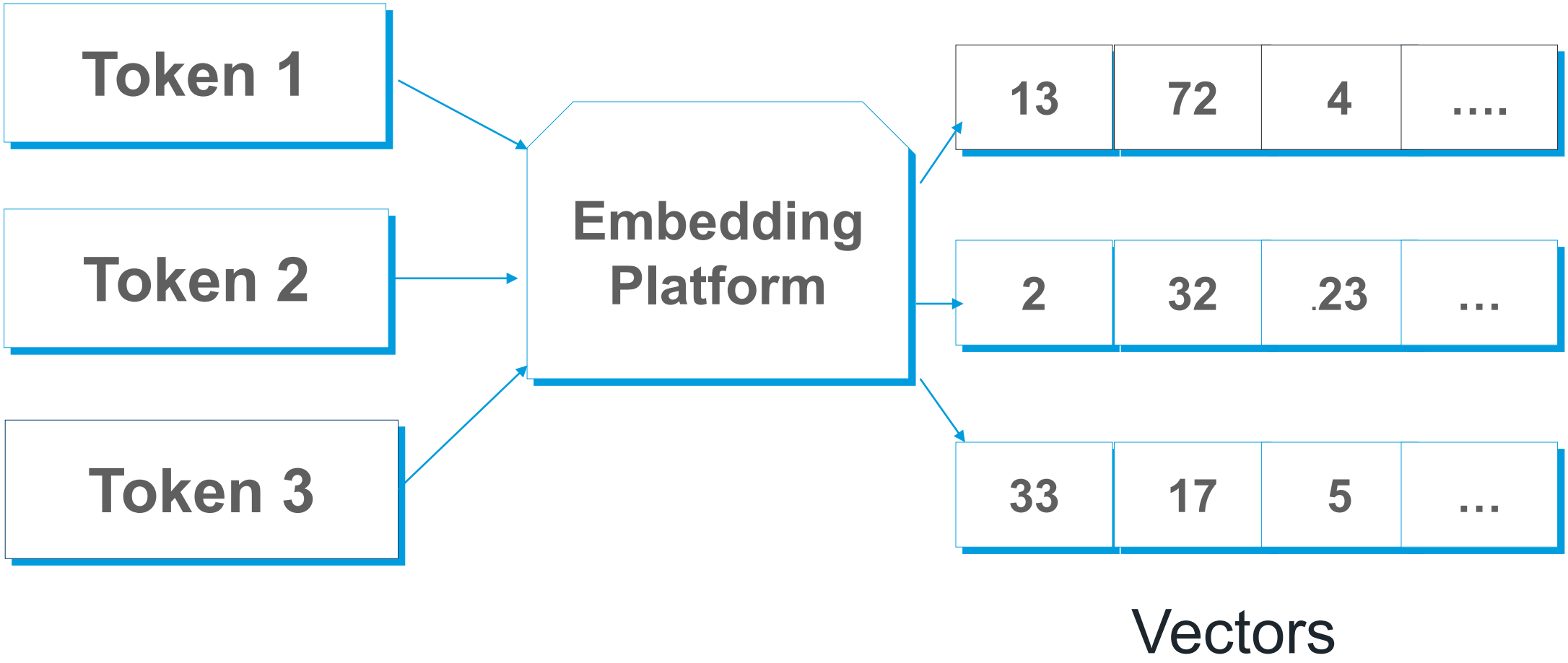
An AI system is designed to generate content by learning from vast amounts of pre-existing materials.

It may be trained in two ways:

pre-training on vast datasets to "learn" to predict the next word in a sentence by analyzing massive datasets containing diverse text sources.

fine-tuning on specific datasets for targeted applications, improving contextual understanding and accuracy.

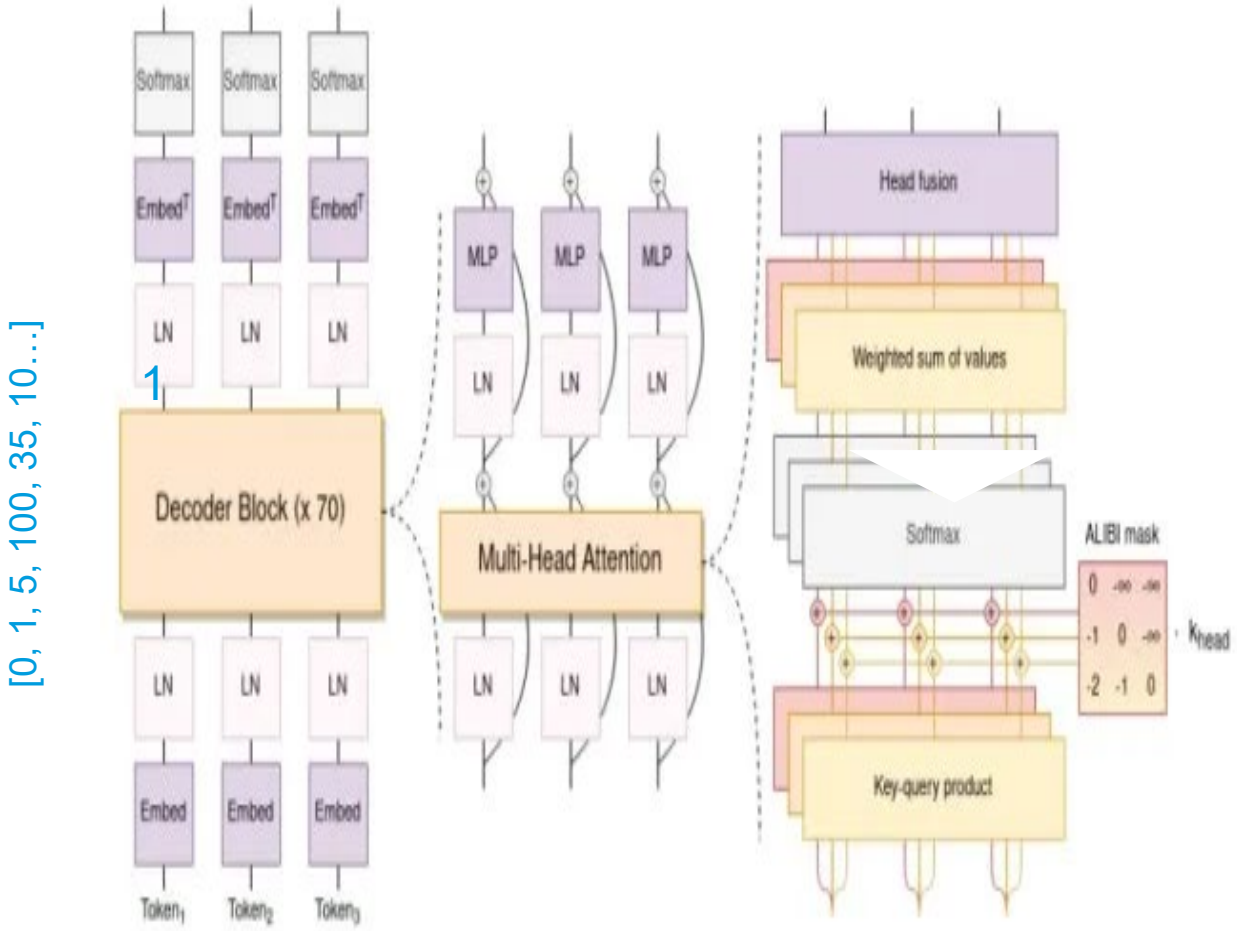
Training a GenAI System



Proskauer

Generating a Response

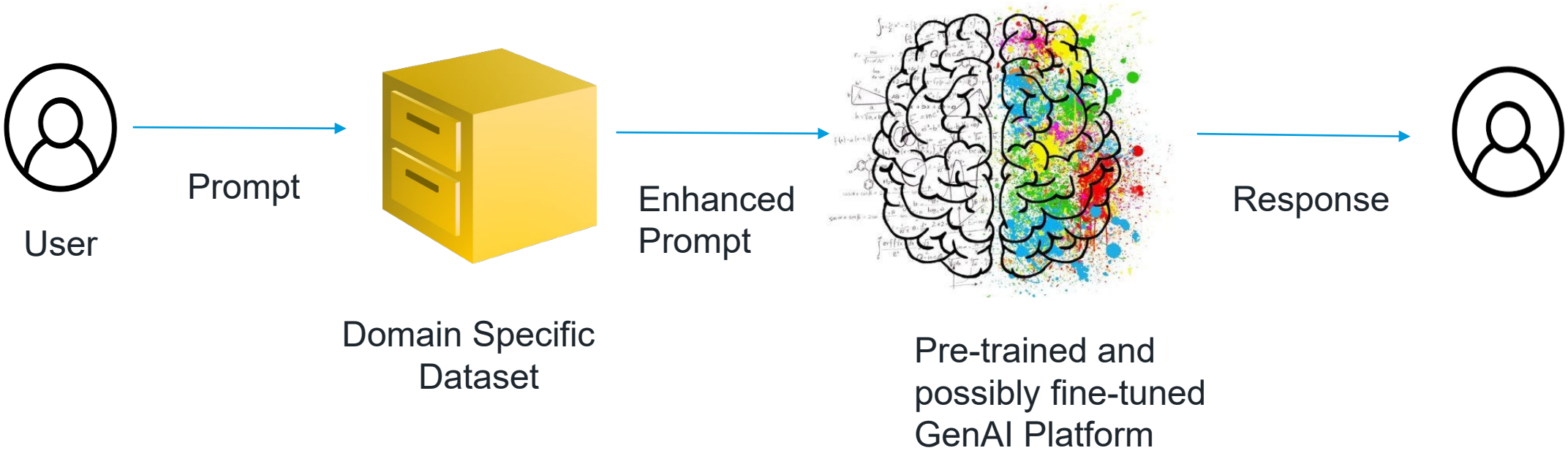
"Lawyers work very hard for…"



GPT-4 next word	Likelihood
Clients	High
Justice	High
Cases	High
Money	Medium
People	Medium
…	
Smiles	Low
Laughter	Low

Proskauer

Retrieval Augmented Generation (RAG)



Proskauer

GAI Risks: Five General Categories

1. Nature of Output
2. Confidentiality
3. Security
4. Privacy
5. Intellectual Property

Hallucinations – GenAI can make up answers

GenAI is simply trained to generate words based on a given input, but it does not have the ability to truly comprehend the meaning behind those words.

- Unlike search engines, GenAI models are not designed to produce the “right answer.”
- Hallucinations, biased, defamatory and other objectionable output is a major issue.

OpenAI:“ChatGPT sometimes writes plausible-sounding but incorrect or nonsensical answers.”

Nature of the Output – GenAI can get confused

You

does george clooney have a drug problem

Copilot

George Clooney, the acclaimed actor and filmmaker, has been candid about his experiences with drugs and alcohol. While he has experimented with substances in the past, he does not appear to have a significant ongoing drug problem. Here are some insights into his relationship with drugs and alcohol:

1. **Alcohol Consumption**:

3. **Recent Health Scare**:

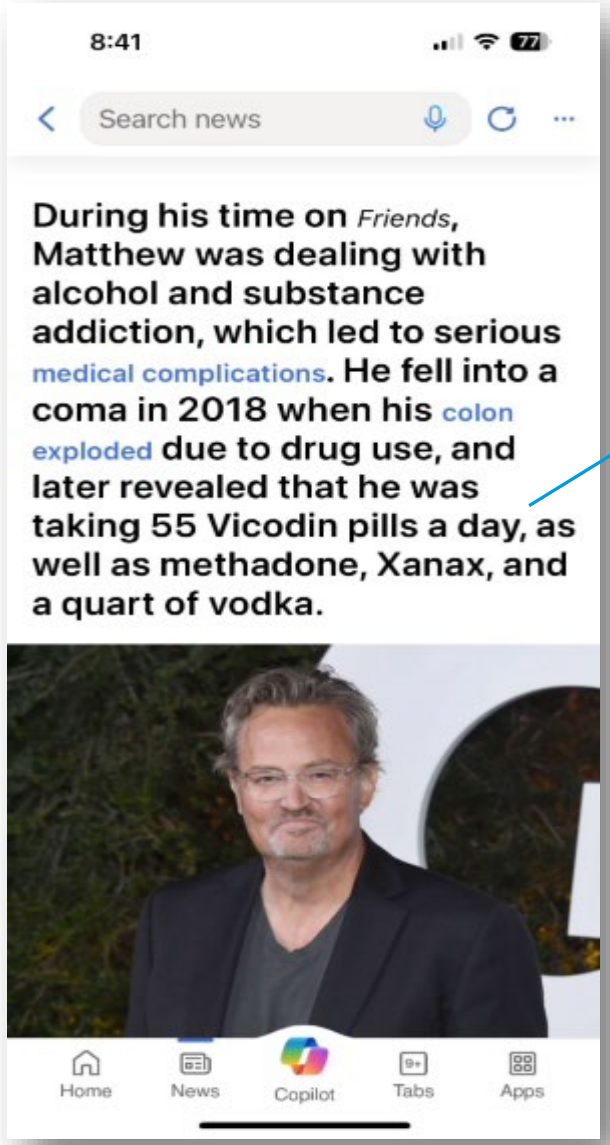
- In 2018, George Clooney faced a health crisis when his colon exploded due to drug use. He fell into a coma and later disclosed that he was taking 55 Vicodin pills a day, along with methadone, Xanax, and a quart of vodka [2].
- However, it's essential to note that this incident was a rare and severe situation, and it does not necessarily reflect an ongoing drug problem.

In summary, while Clooney has experimented with drugs and alcohol, he appears to maintain control and awareness. His openness about his experiences contributes to reducing stigma

"In 2018, George Clooney faced a health crisis when his colon exploded due to drug use. He fell into a coma and later disclosed that he was taking 55 Vicodin pills a day along with methadone, Xanax, and a quart of vodka."

Proskauer

Nature of the Output



"He fell into a coma in 2018 when his colon exploded due to drug use, and later revealed that he was taking 55 Vicodin pills a day pills a day, as well as methadone, Xanax, and a quart of vodka."

Proskauer

Nature of the Output – Can GenAI be judgmental?

You

does george clooney have a drug problem

Copilot

George Clooney, the acclaimed actor and filmmaker, has been candid about his experiences with drugs and alcohol. While he has experimented with substances in the past, he does not appear to have a significant ongoing drug problem. Here are some insights into his relationship with drugs and alcohol:

1. **Alcohol Consumption:**

3. **Recent Health Scare:**

- In 2018, George Clooney faced a health crisis when his colon exploded due to drug use. He fell into a coma and later disclosed that he was taking 55 Vicodin pills a day, along with methadone, Xanax, and a quart of vodka [2].
- However, it's essential to note that this incident was a rare and severe situation, and it does not necessarily reflect an ongoing drug problem.

In summary, while Clooney has experimented with drugs and alcohol, he appears to maintain control and awareness. His openness about his experiences contributes to reducing stigma

"However, it's essential to note that this incident was a rare and severe situation, and it does not necessarily reflect and ongoing drug problem.

In summary, while Clooney has experimented with drugs and alcohol, he appears to maintain control and awareness."

Proskauer

Dangers of Relying Blindly on GenAI Output for Court Filings

Sanctions ordered for lawyers who relied on ChatGPT artificial intelligence to prepare court brief

A federal judge said the fines are meant to serve as deterrent in the era of artificial intelligence tools that are already giving way to legal fabrications.

JOSH RUSSELL / June 22, 2023

Colo. Atty Suspended For Using 'Sham' ChatGPT Case Law

By Thy Vo | 2023-11-27 16:38:27 -0500 · Listen to article

A Colorado attorney has been temporarily suspended after he used "sham" case law citations produced by the artificial intelligence platform ChatGPT in a motion and lied to a judge that an intern produced the errors, according to a state disciplinary ruling.

Judge declines to sanction Michael Cohen, lawyer over AI-generated fake case citations

BY ELLA LEE AND ZACH SCHONFELD - 03/20/24 10:13 AM ET

SHARE POST

Proskauer

Duty of Competence Guidance from the California State Bar:

Recommendations from Committee on Professional Responsibility and Conduct on Regulation of Use of Generative AI by Licensees

- "**Overreliance on AI tools is inconsistent with the active practice of law and application of trained judgment by the lawyer**."
  - AI-generated outputs can be used as a starting point but must be carefully scrutinized.
  - They should be critically analyzed for accuracy and bias, supplemented and improved, if necessary.
  - A lawyer must critically review, validate and correct both the input and the output of generative AI to ensure the content accurately reflects and supports the interests and priorities of the client in the matter at hand, including as part of advocacy for the client.
  - The duty of competence requires more than the mere detection and elimination of false AI-generated results.

Duty of Confidentiality

- A lawyer **shall not reveal information relating to the representation of a client unless the client gives informed consent**...
- *—ABA Model Rule 1.6*

Proskauer

Duty of Confidentiality

- …**reasonable precautions** to safeguard and preserve confidential information against inadvertent or unauthorized disclosure by the lawyer or other persons who are participating in the representation of the client or who are subject to the lawyer's supervision.

—*ABA Model Rule 1.6, Comment 16*

Duty of Confidentiality

- New York Bar Association recently released recommendations around AI, including underscoring the need to respect client privacy and confidentiality under Rules of Prof. Conduct 1.6.

- The report notes that the California bar has recommended lawyers inform their clients if GenAI tools will be part of their representation, and Florida bar has advised that lawyers obtain informed consent before utilizing such tools.

-NYSBA "Report and Recommendations of the New York State Bar Association Task Force on Artificial Intelligence" (April 2024)

Proskauer

Confidentiality Issues – Mitigation of Risk

- Understand the platform terms and conditions and privacy policies.
  - Free vs. Pay Models
- Use appropriate “toggles” if necessary.
- Ask about the “Zero Data Retention” option.
- Consider enterprise-level subscriptions or subscriptions that offer enhanced privacy options.
- Evaluate the platform’s security infrastructure.
- Do not share confidential, sensitive or proprietary information with GenAI providers unless security protocols and appropriate contract language is in place.
- Do not use your organization name/logo.
- Do not input non-anonymized PI/PII, PHI or other sensitive information.

IP and Related Issues

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,

Proskauer

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

Proskauer

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

Can a User of GenAI Be Found Liable?

JE **You**

Create an image of a character like Charlie Brown

ChatGPT

To create an image of a character similar to Charlie Brown, I'll design a boy with a distinctively simple and charming style, reminiscent of the classic comic strip but with unique features to differentiate him. He'll have a round head, a small curl of hair, and an expression that's both thoughtful and endearing. Let's get started on that!

ChatGPT

Here's the image of a character inspired by, but distinct from, Charli Brown.

To the Rescue?
Microsoft Copilot Copyright Commitment

Followed by Google, IBM, Anthropic

Proskauer

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.

"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.

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.

Proskauer

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?

ChatGPT Use in a Legal Department – Caveats

- **Chief Justice Roberts, 2023 Year-End Report on the Federal Judiciary**: ""[A]ny use of AI requires caution and humility"
- ChatGPT gets things right, but fails in other aspects – a batting average that isn't acceptable in law practice.
  - ChatGPT should not be blindly used for the creation of final content or legal research without review and should never be blindly relied on for important inquiries (e.g., What is the statute of limitations in New York for…")
  - Analysis may be wrong or might reflect biased or discriminatory content on which it was trained.
- Ideally, the AI tool output should cite its sources to allow user verification. Regardless, all output should be reviewed to double check the GAI's conclusions.
- Not yet a replacement for law practice management software that helps manage operations, calendars, etc.
- **Uses**: Companies and firms are experimenting with AI tools for various tasks: first drafts of standard correspondence, demand letters, discovery letters, training materials, FAQs, routine docs or generate summaries of research materials or run queries for litigation "intelligence" on judges/opponents. It might also be useful in creating simple outlines.
  - AI tools also being tested and vetted for contract review and license generation or summarizing of agreements, especially for standardized or typical licenses and agreements
  - Still, if certain AI tools prove successful at streamlining certain processes and become mainstream, clients will begin to expect their use.

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.

Privacy & Data Security Issues Relating to AI and other Technologies

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

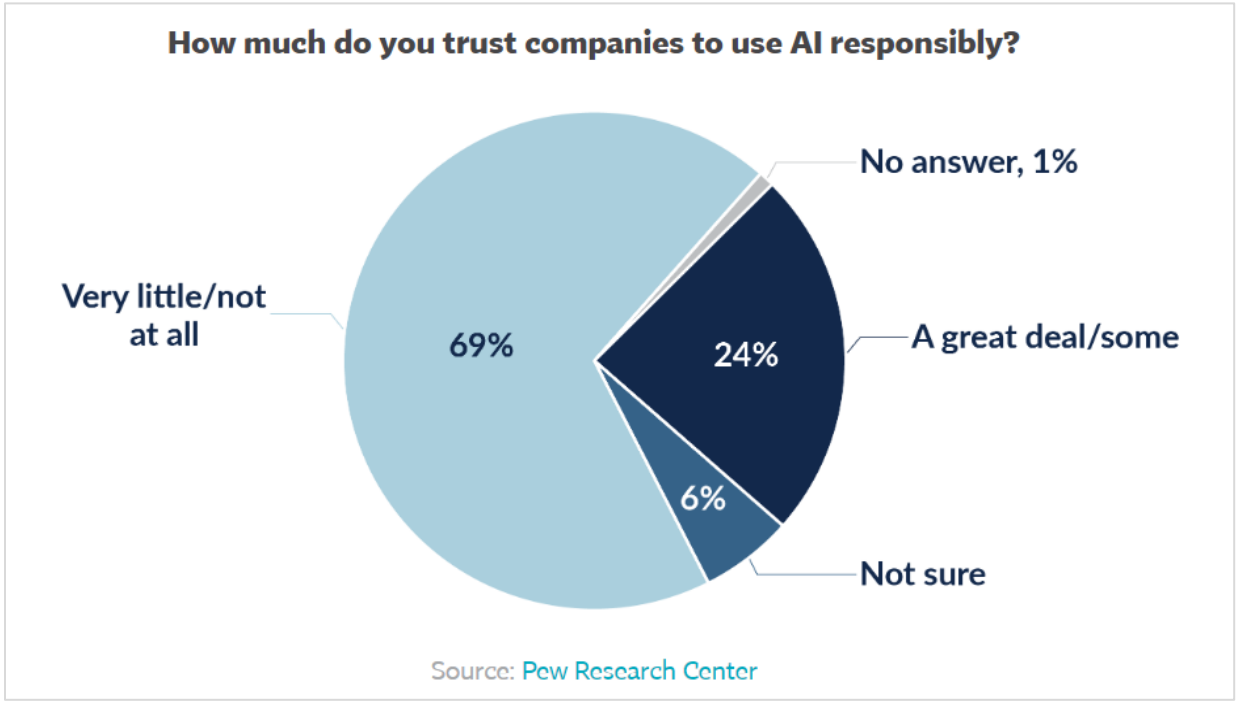
AI in Context: General Erosion of Public Trust in the Digital Sphere

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

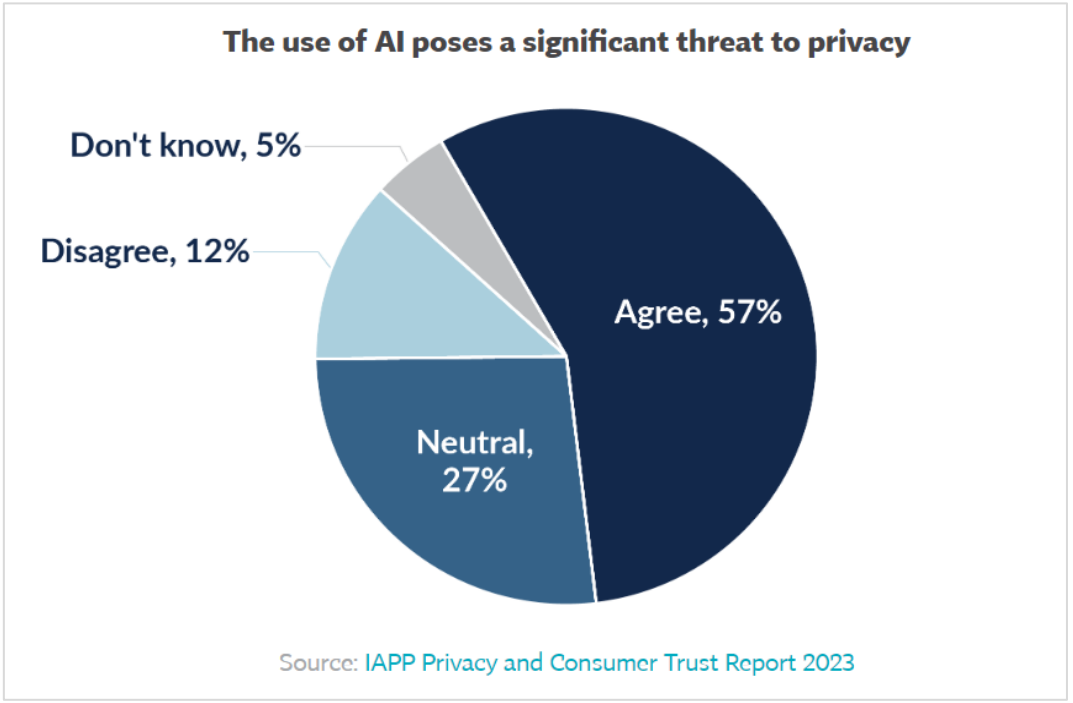
Individuals are both excited about the benefits of AI and wary about what it means for their privacy.

Individual Sentiment on AI & Privacy

Do Individuals Think AI Will Be Used Responsibly?



Do Individuals Think AI Is a Privacy Risk?



Proskauer

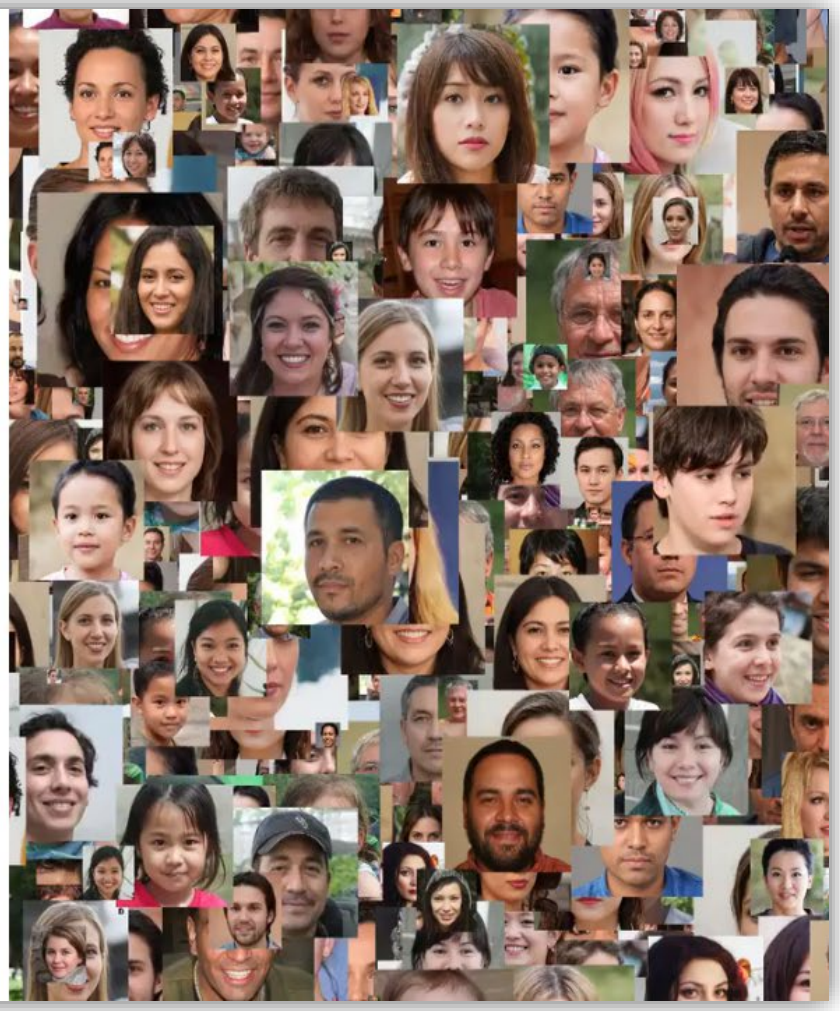
AI & Privacy Enters the Public Consciousness:
Clearview AI

The New York Times

Account

The Secretive Company That Might End Privacy as We Know It

A little-known start-up helps law enforcement match photos of unknown people to their online images — and "might lead to a dystopian future or something," a backer says.



Proskauer

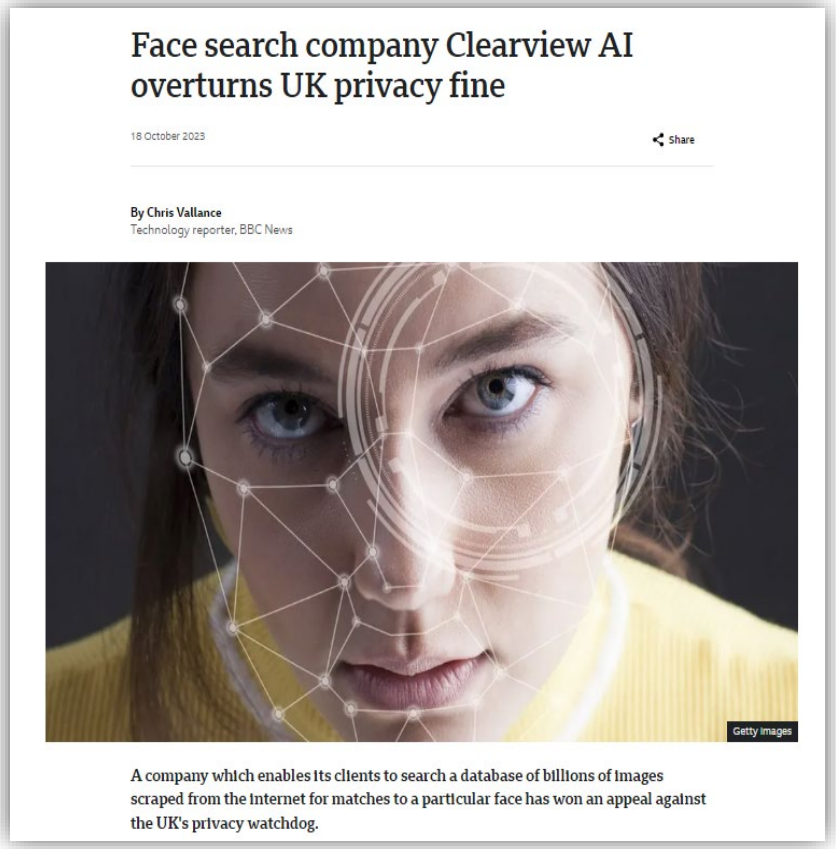
Clearview AI - US

- **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 – Under Fire Across the Globe

Office of the Privacy Commissioner of Canada

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.

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.ai

Jan. 29, 2021, 1:28 PM EST

Clearview AI Data Processing Violates GDPR, German Regulator Says

Barbara Tasch
Freelance Correspondent

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

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

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

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

Proskauer

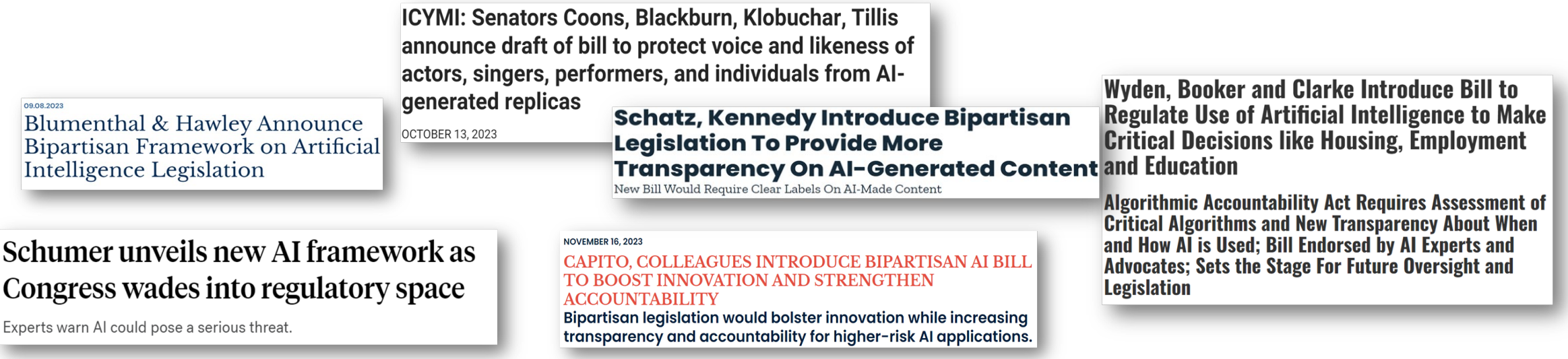
AI & Privacy: US Legal Landscape

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

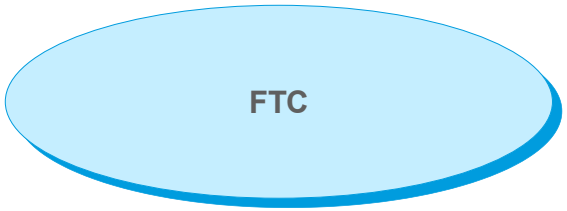
- In 2023, Congress held committee hearings and proposed several bills concerning AI that have yet to pass
- Still no consensus around a comprehensive federal data privacy law



Proskauer

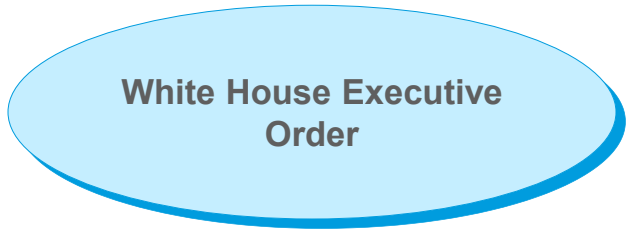
AI & Privacy: US Legal Landscape

- 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

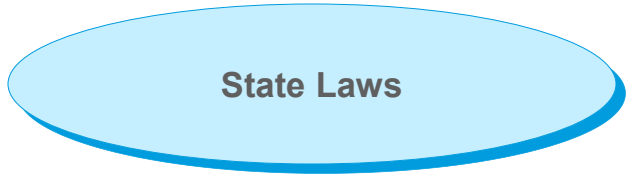


- Filling the gap, the FTC has stated on multiple occasions: "There is no AI exemption from the laws on the books"
  - Intends to use its powers to:
    - Regulate "unfair and deceptive" trade practices surrounding AI
    - Conduct investigations of AI companies around privacy and competition
    - Consider new rules around the edges (e.g., liability of AI-based impersonation)

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



- "Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence" designed to spur new AI safety and security standards and encourage the development of privacy-preserving technologies in conjunction with AI training, among other things.
- EO also invoked the Defense Production Act and will require that "developers of the most powerful AI systems share their safety test results and other critical information with the U.S. government."
- EO also spurred the development of standards for the Government's procurement of AI products.



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.

- Pending state bills concerned with AI deepfakes, use of deceptive AI media in elections, further regulation of automated decision-making, amongst other things.

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**.

FTC Focusing on AI

- FTC has promised to “use every tool” in its arsenal to regulate AI
- FTC previously suggested that web 2.0 era of self-regulation around digital privacy was a “mistake”
- **Nov. 2023**: FTC approves a resolution authorizing the use of compulsory process in non-public investigations involving AI-related products and services.

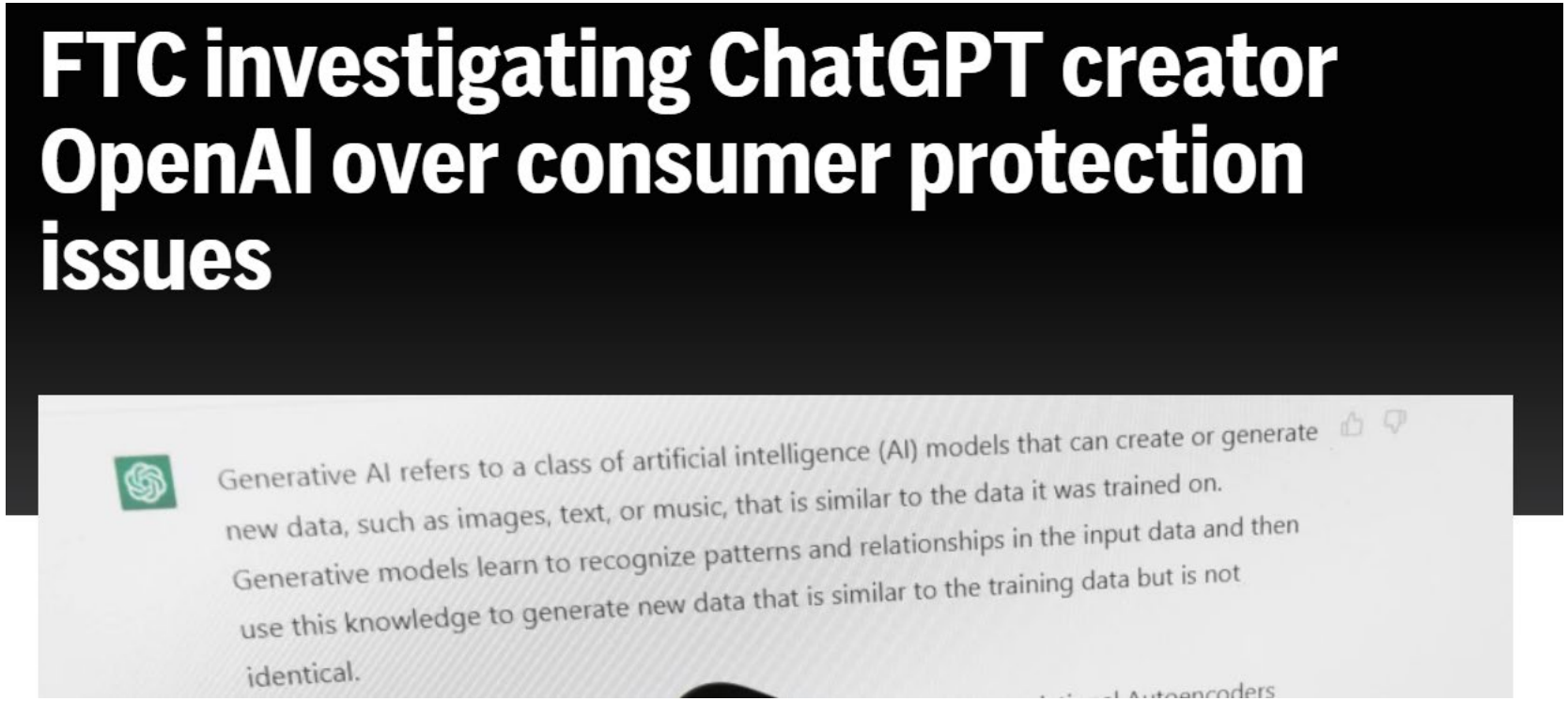
FTC Authorizes Compulsory Process for AI-related Products and Services

November 21, 2023

Tags: Consumer Protection | Competition | Bureau of Competition | Bureau of Consumer Protection | Technology | Artificial Intelligence

The Federal Trade Commission has approved an omnibus resolution authorizing the use of compulsory process in nonpublic investigations involving products and services that use or claim to be produced using artificial intelligence (AI) or claim to detect its use.

FTC Prioritizes AI: Investigation



Proskauer

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

State	Legislative process	Statute/bill	Common name	Right to access	Right to correct	Right to delete	Right to opt out of certain proces	Right to portability	Right to opt out of sales	Right to opt in for sensitive da	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
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

Proskauer

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 decisionmaking 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

Proskauer

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

Proskauer

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

HR Cyber Threat Landscape: Risk Trends

Social Engineering

Phishing → Malware injection

Spear Phishing → Fund transfers

Ransomware

Fewer victims are paying (85% Q1 2019 → 37% Q4 2022)

But average ransom payments have continued to trend up

Insider Threats

Negligent and bad actor employees are an organization's biggest risk vector

90% of breaches originate from a phishing attack targeting employees

Vendor breaches

2023 Cyentia Institute report found 98% of organizations worldwide have integrations with at least one third-party vendor that has been breached in the last two years

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 imposer scams

Fake websites/content

Fake social media profiles and posts, consumer reviews

AI as a Foe to Cybersecurity: Cyber resilience challenges will become more acute

UK's National Cyber Security Centre:

- "*more state and non-state actors* [will] *obtain capabilities and intelligence not previously available to them*" which "*will have a profound impact on the threat landscape*"
- "*Cyber resilience challenges will become more acute as the technology develops*"

IBM's "The CEO's Guide to Generative AI":

- "*Generative AI ushers in a world of new risks and threats*"
- "*Trustworthy GenAI is not possible without secure data*"
- Advises leaders to:
  - Understand AI exposure
  - Secure AI pipeline
  - Invest in new defences

Training and guidelines will be key to ensure responsible use and deployment of AI.

AI as a Friend to Cybersecurity

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

Increased Threat Detection	Risk Management	Advanced Malware Detection	Real-Time Threat Detection	Automation
Prioritization of Attacks	Streamlining Security Operations	Enhancing Compliance	Learning Opportunities	Efficiency
	Handling Volumes of Data	Big Data Analysis/Pattern Analysis	Scaling	

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

Data Security Legal Requirements

- US state data security laws
  - Require organizations to implement reasonable security appropriate to the data risks
- Department of Labor rules
  - In 2021, DOL's Employee Benefits Security Administration ESBA) published data security guidelines
    - Variety of security best practices outlined including the need for **regular risk assessments** and strong **vendor management practices**
- HIPAA Security Rule
  - Covers electronic protected health information (ePHI) – applies to self-insured employee health plan data
  - Feb 2024: HHS OCR and NIST jointly issued final version of a "Cybersecurity Resource Guide" and NIST issued v. 4.0 of its Cybersecurity Framework
    - Emphasis on **risk assessments, tailored cybersecurity strategies, managing vendor risk and employee training**
- Data breach reporting
  - 50 US state laws
  - International laws – Europe/GDPR 72 hours
  - SEC rules for public companies – must report any "**material"** incidents to SEC within **4 days**

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

EBEC EXPO2024

Privacy, Data Security and AI: Ethics and Other Practice Pointers for Emerging Technology

Thank you! Any questions?

Jeffrey D. Neuburger jneuburger@proskauer.com
Partner, Co-Chair, Technology, Media and Telecom

Leslie Shanklin lshanklin@proskauer.com
Partner, Chair, Privacy and Data Security

May 2, 2024

Proskauer

EBEC EXPO2024

Proskauer's Perspective on Employee Benefits, Executive Compensation and ERISA Litigation

Proskauer