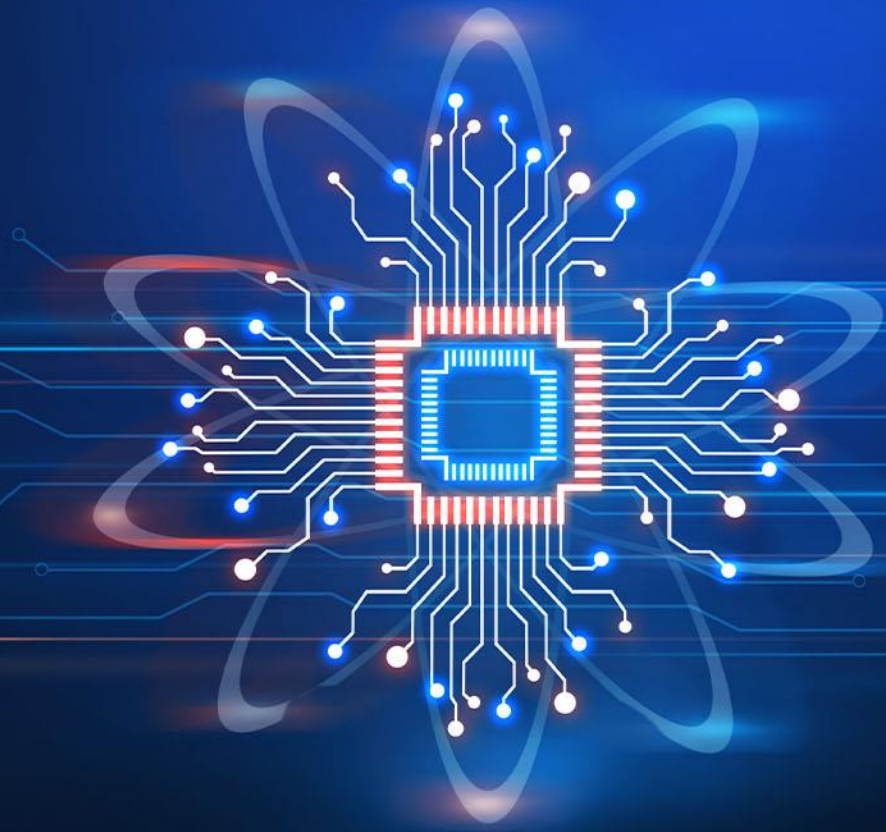
A Proskauer Webinar Series

The Age of AI



Data Privacy & Security

Leslie Shanklin, Partner
Kelly McMullon, Special Counsel

Proskauer

Privacy & Security Considerations in the Context of AI

- Data Privacy & Security Impacts
  - Clearview AI Enforcement
- USA Update
  - US Legal Landscape
  - FTC
  - Litigation
  - Privacy Compliance
- EU Update
  - Enforcement Action
  - AI Act
- Other Updates & Approaches
  - Global Developments
  - UK
  - Canada
- AI Privacy Risk Management Strategies
- AI & Cybersecurity
- A Silver Lining? Beneficial Uses of AI for Privacy and Security Protection

Data Privacy & Security Impacts of AI

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?

Proskauer

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*: Medical data a hospital collects for medical care being used for medical diagnosis

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

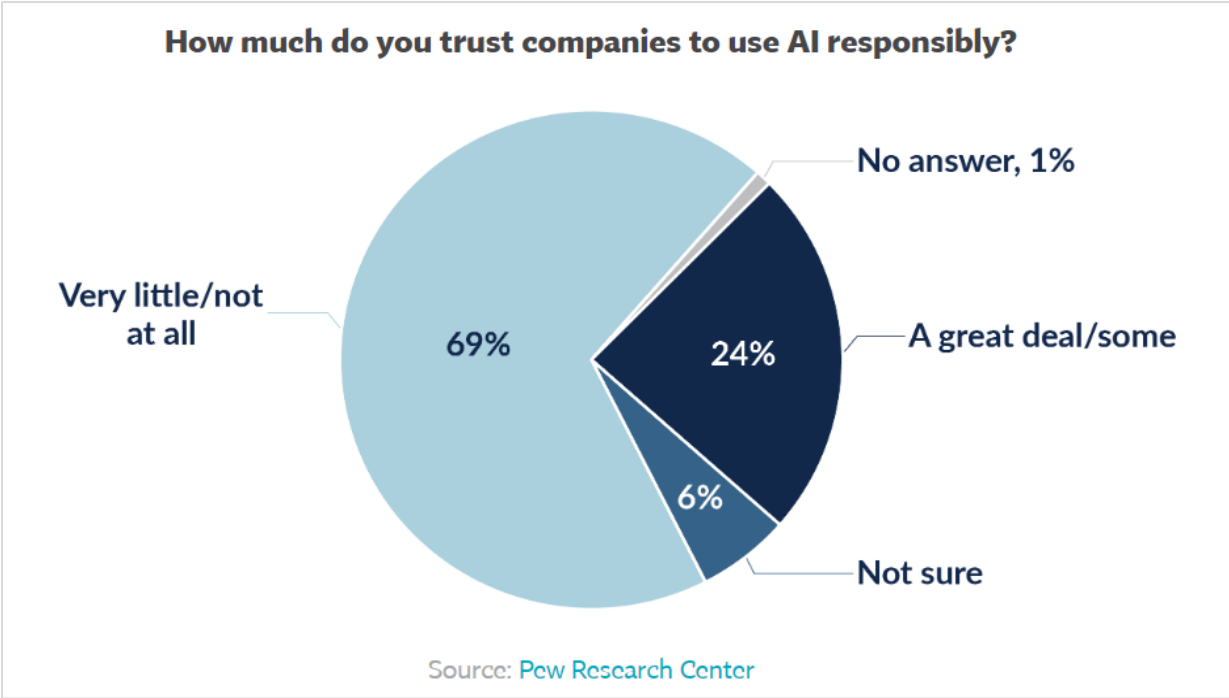
AI in Context: Erosion of Public Trust in the Digital Sphere

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

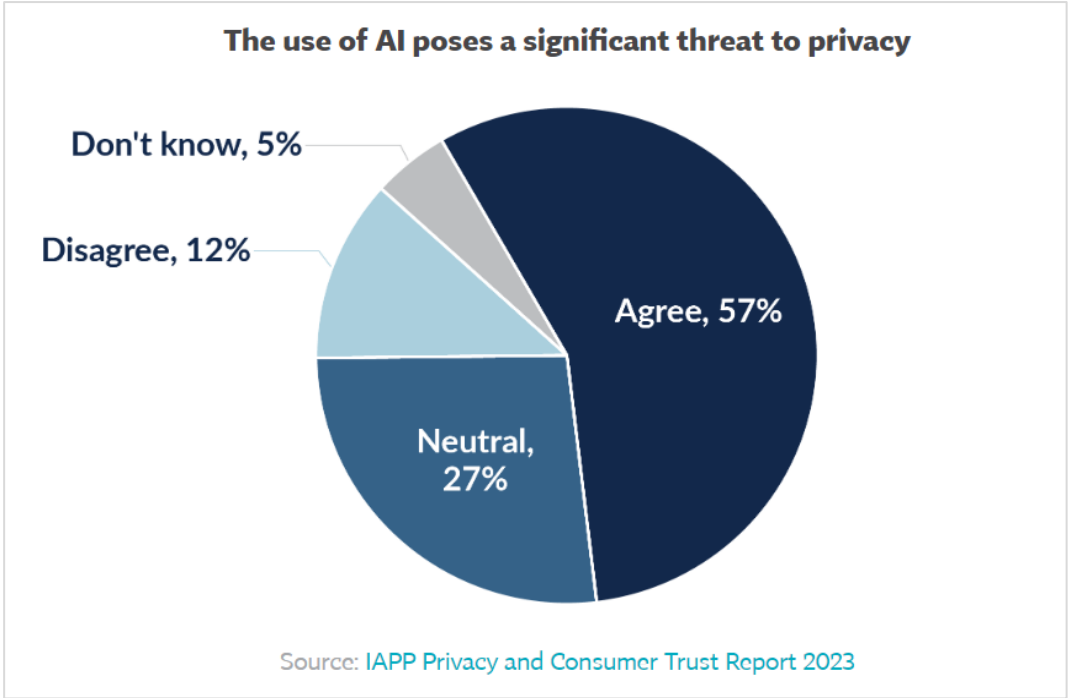
Consumers are both excited about the benefits of AI and wary about what it means for their privacy.

Consumer Sentiment on AI & Privacy

Do Consumers Think AI Will Be Used Responsibly?



Do Consumers Think AI Is a Privacy Risk?



Proskauer

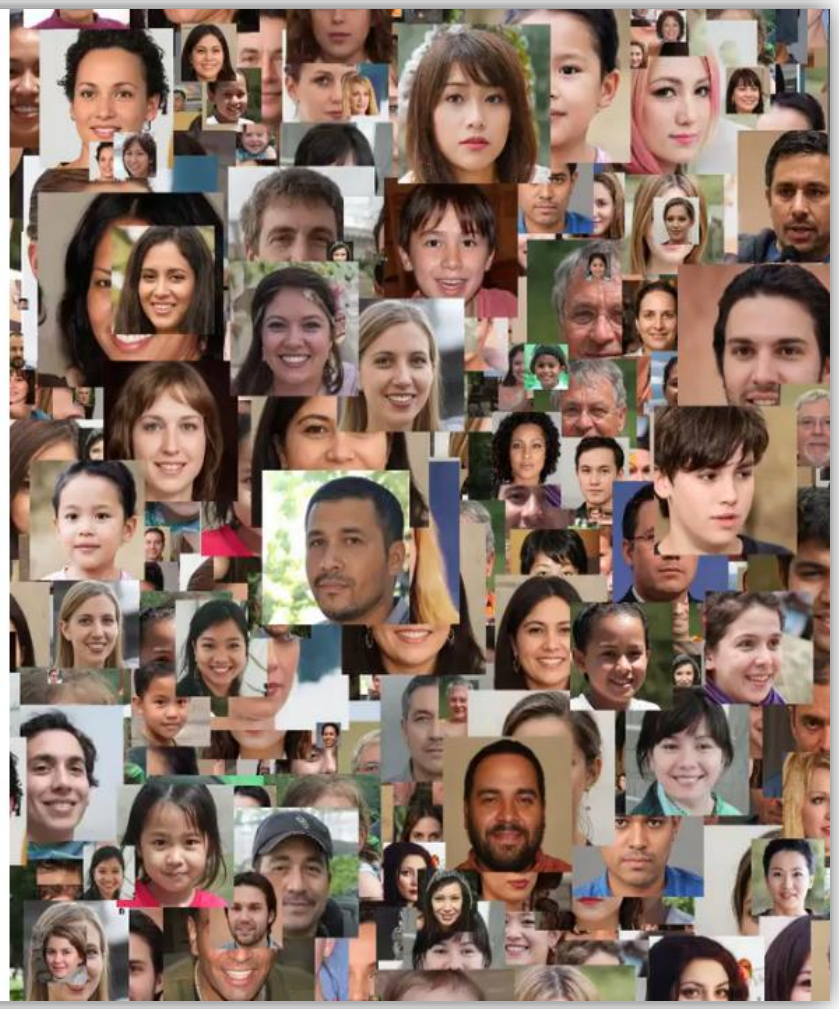
AI & Privacy Enters the Public Consciousness:
Clearview AI

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.

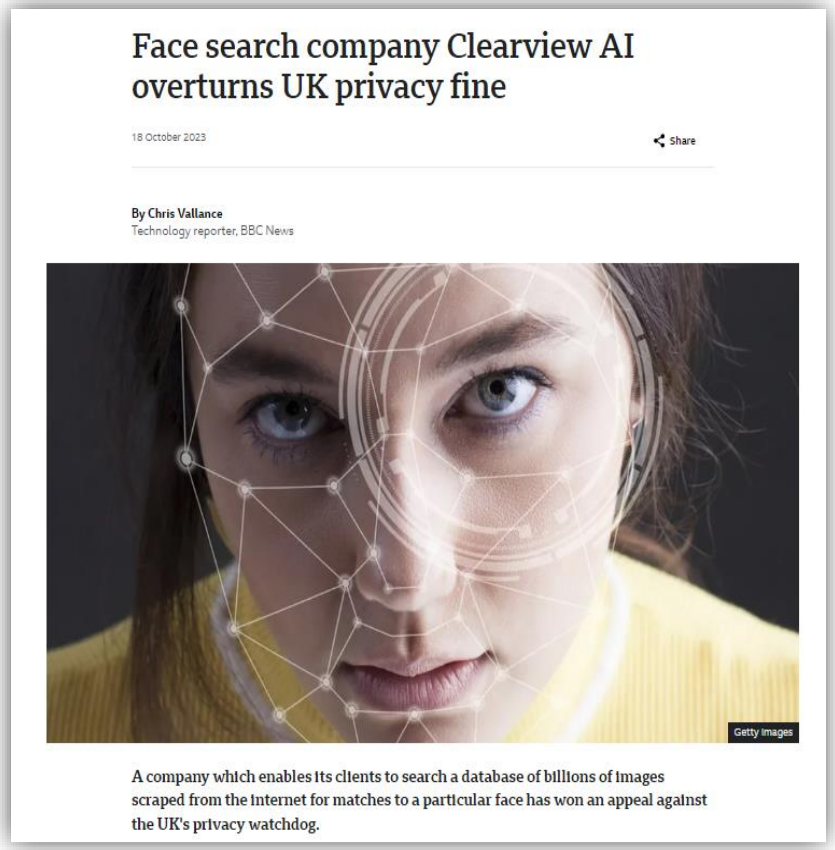
In other U.S. litigations, Clearview has thus far been unsuccessful in advancing its argument that it has a First Amendment right to collect "public data".

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 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

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 Update

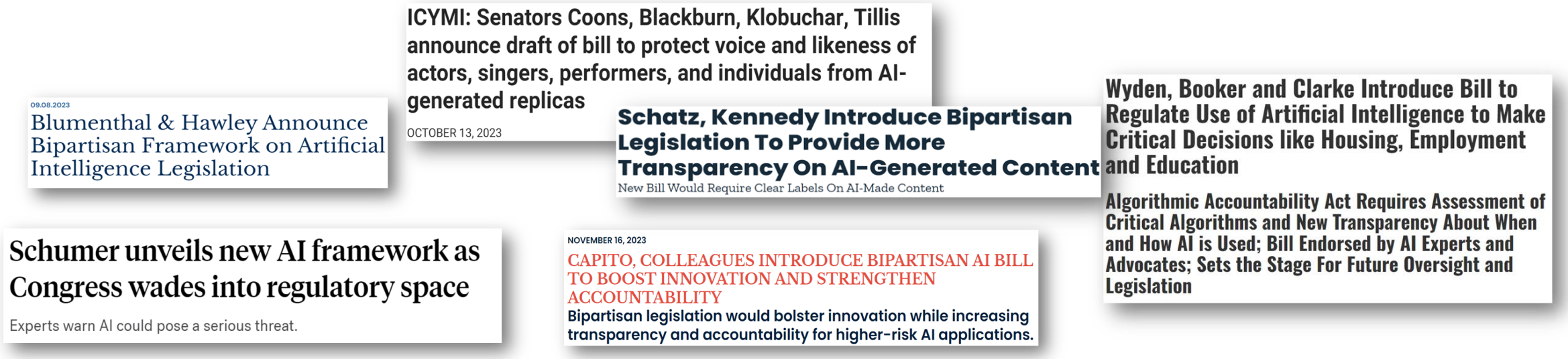
AI & Privacy: US Legal Landscape

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 Federal Law

- 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

FTC

- 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)

State Laws

- ***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.
    - Laws give consumers the right to opt-out of "profiling" if it furthers a system's automated decision-making processes in a way that produces "legal or other similar significantly effects" (e.g., unfair or deceptive treatment of consumers; negative impacts on an individual's physical or financial health; provision of financial and lending services, housing, insurance or education)

- ***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.

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: Enforcement

Rite Aid Banned from Using AI Facial Recognition After FTC Says Retailer Deployed Technology without Reasonable Safeguards

FTC says Rite Aid technology falsely tagged consumers, particularly women and people of color, as shoplifters; Ban will last five years

December 19, 2023

Tags: Consumer Protection | Bureau of Consumer Protection | Retail | Privacy and Security | Tech | Artificial Intelligence

Rite Aid will be prohibited from using facial recognition technology for surveillance purposes for five years to settle Federal Trade Commission charges that the retailer failed to implement reasonable procedures and prevent harm to consumers in its use of facial recognition technology in hundreds of stores.

Related Cases

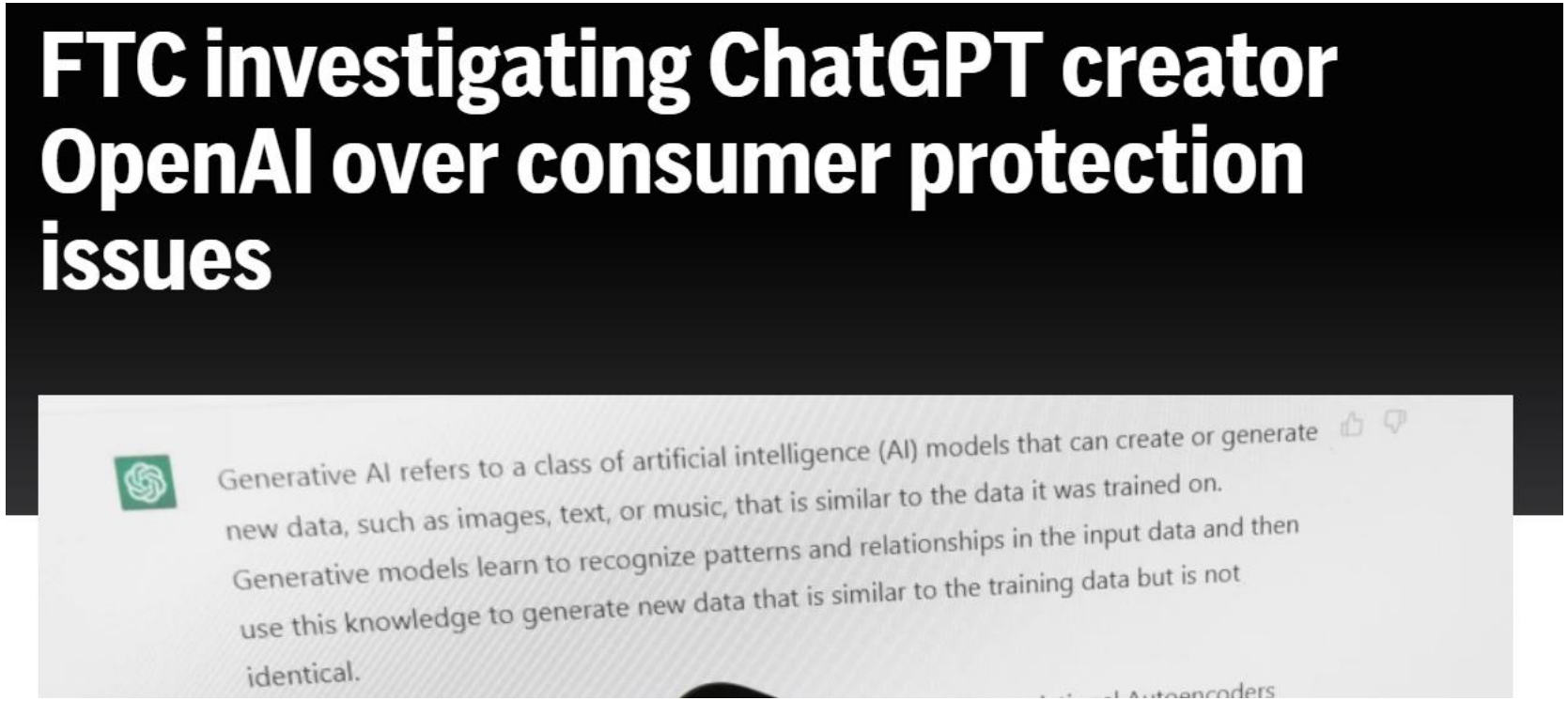
Rite Aid Corporation, FTC v.

Rite Aid Corporation, In the Matter

Related actions

Proskauer

FTC Prioritizes AI: Investigation



Proskauer

FEDERAL TRADE COMMISSION ("FTC")
CIVIL INVESTIGATIVE DEMAND ("CID") SCHEDULE
FTC File No. 232-3044

I. SUBJECT OF INVESTIGATION

Whether "the "Company," as defined herein, in connection with offering or making available products and services incorporating, using, or relying on Large Language Models has (1) engaged in unfair or deceptive privacy or data security practices or (2) engaged in unfair or deceptive practices relating to risks of harm to consumers, including reputational harm, in violation of Section 5 of the FTC Act, 15 U.S.C. § 45, and whether Commission action to obtain monetary relief would be in the public interest. See also attached resolution.

15. Describe in Detail the data You have used, during or prior to the Applicable Time Period, to train or otherwise develop each Large Language Model described in response to Interrogatory 9, including, for each such model:

    a. How You obtained the data, e.g., by scraping the data, purchasing it from third parties, or by other means;

    b. All sources of the data, including any third parties that provided data sets;

22. Describe in Detail the steps that the Company takes, if any, to prevent Personal Information or information that may become Personal Information when combined with other information in the training data from being included in the training data for any Large Language Model(s). Include in Your response a description of any mechanisms, processes, and/or procedures for removing, filtering, anonymizing, or otherwise obscuring such data.

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

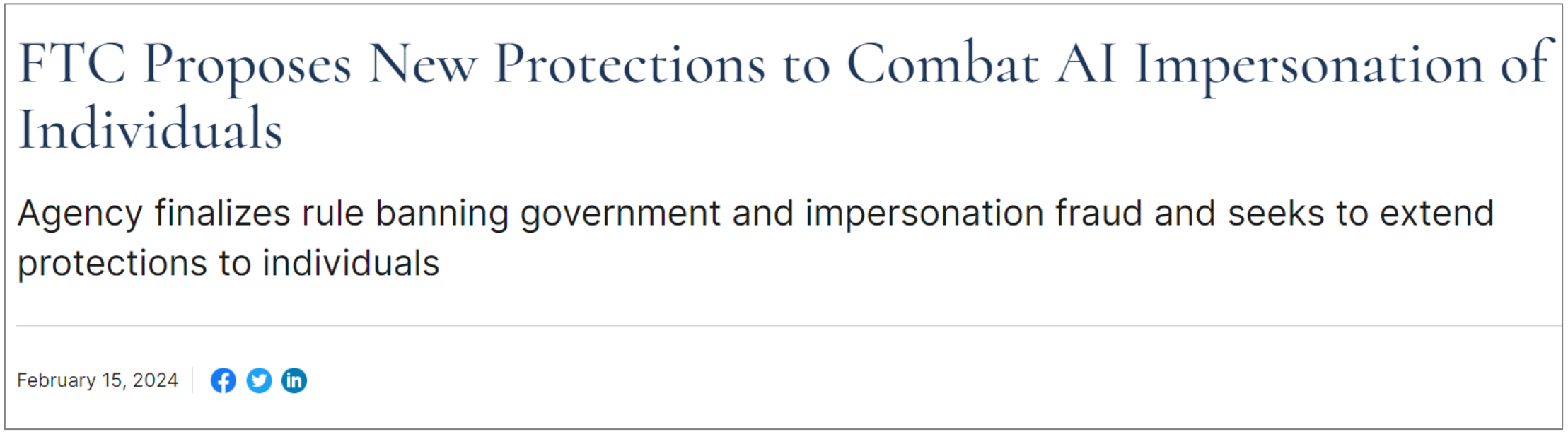
AI (and other) Companies: Quietly Changing Your Terms of Service Could Be Unfair or Deceptive

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."

FTC Rulemaking



FTC Proposes New Protections to Combat AI Impersonation of Individuals

Agency finalizes rule banning government and impersonation fraud and seeks to extend protections to individuals

February 15, 2024

Statement of Chair Lina Khan: "**In its supplemental NPRM, the Commission proposes to expand the rule's prohibitions to also cover impersonation of individuals**. If adopted, this additional protection will equip enforcers to seek civil penalties and redress when fraudsters impersonate individual people, not just government or business entities. **Given the proliferation of AI-enabled fraud, this additional protection seems especially critical. Notably, the supplemental proposal also recommends extending liability to any actor that provides the "means and instrumentalities" to commit an impersonation scam.** Under this approach, liability would apply, for example, to a developer who knew or should have known that their AI software tool designed to generate deepfakes."

FCC Rulemaking - Robocalls

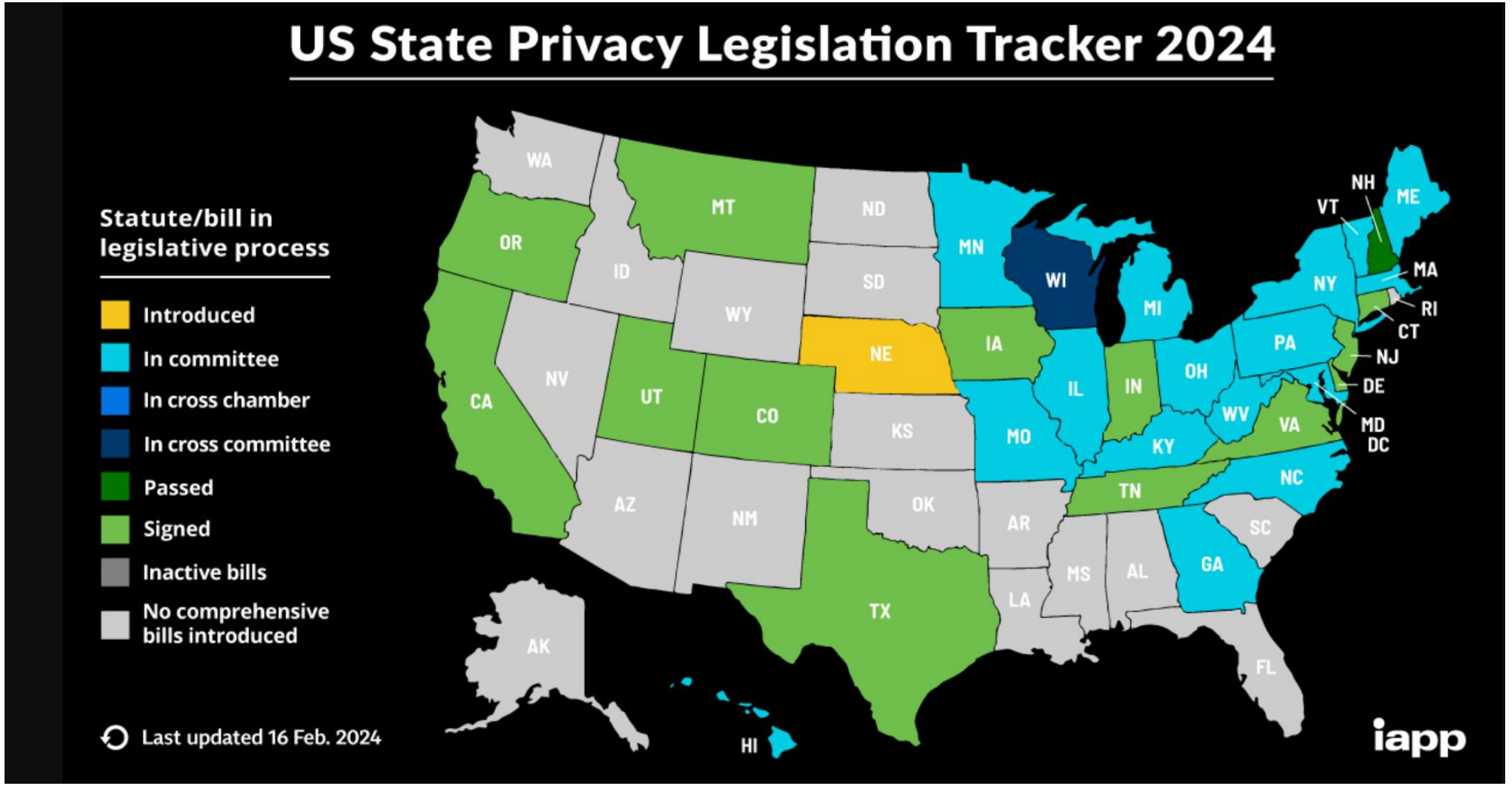
- Declaratory Ruling that recognizes calls made with AI-generated voices are “artificial” under the Telephone Consumer Protection Act (TCPA).
- The ruling, which takes effect immediately, makes voice cloning technology used in common robocall scams targeting consumers illegal.

FCC MAKES AI-GENERATED VOICES IN ROBOCALLS ILLEGAL

State AGs Will Now Have New Tools to Go After Voice Cloning Scams

WASHINGTON, February 8, 2024—Today the Federal Communications Commission announced the unanimous adoption of a Declaratory Ruling that recognizes calls made with AI-generated voices are “artificial” under the Telephone Consumer Protection Act (TCPA). The ruling, which takes effect immediately, makes voice cloning technology used in common robocall scams targeting consumers illegal. This would give State Attorneys General across the country new tools to go after bad actors behind these nefarious robocalls.

State Privacy Laws



Proskauer

State Privacy Laws – Automated Decisionmaking

US State Privacy Legislation Tracker 2024

iapp

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 proc	Right to portability	Right to opt out of sales	Right to opt in for sensitiv 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
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

California: CCPA Regulations on Automated Decisionmaking

- California Privacy Protection Agency (CPPA) met in January to discuss draft regulations on automated decisionmaking issued in Nov 2023 Draft Automated Decisionmaking Technology Regulations (ca.gov)

- Regs would require businesses using automated decisionmaking technology (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

State Legislatures Keenly Focused on AI

Scoop: N.Y. governor wants to criminalize deceptive AI

Ryan Heath, author of Axios AI+

New York Gov. Kathy Hochul. Photo: John Lamparski/Getty Images

New York Gov. Kathy Hochul is proposing legislation that would criminalize some deceptive and abusive uses of AI and require disclosure of AI in election campaign materials, her office tells Axios.

States turn their attention to regulating AI and deepfakes as 2024 kicks off

Since the beginning of the year, lawmakers in at least 14 states have introduced legislation to combat the threats AI and deepfakes can pose to political campaigns.

SENATOR WIENER INTRODUCES LEGISLATION TO ENSURE SAFE DEVELOPMENT OF LARGE-SCALE ARTIFICIAL INTELLIGENCE SYSTEMS AND SUPPORT AI INNOVATION IN CALIFORNIA

Task force: Transparency, innovation and safety are key to developing AI in Connecticut

By Ken Dixon, *Staff Writer*
Jan 24, 2024

Proskauer

Litigation

P.M. et al. v. OpenAI LP, No. 23-03199 (N.D. Cal. Filed June 2023)

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

PLAINTIFFS P.M., K.S., B.B., S.J., N.G., C.B., S.N., J.P., S.A., L.M., D.C., C.L., C.G, R.F., N.J., and R.R., individually, and on behalf of all others similarly situated,

Plaintiffs,

vs.

OPENAI LP, OPENAI INCORPORATED, OPENAI GP, LLC, OPENAI STARTUP FUND I, LP, OPENAI STARTUP FUND GP I, LLC, OPENAI STARTUP FUND MANAGEMENT LLC, MICROSOFT CORPORATION and DOES 1 through 20, inclusive,

Defendants.

Case No.:

CLASS ACTION COMPLAINT

1. VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. §§ 2510, *et seq.*
2. VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030
3. VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA"), CAL. PENAL CODE § 631
4. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, BUSINESS AND PROFESSIONS CODE §§ 17200, *et seq.*

CLASS ACTION COMPLAINT

- VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. §§ 2510, et seq.
- 2. VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030
- 3. VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA"), CAL. PENAL CODE § 631
- 4. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, BUSINESS AND PROFESSIONS
- 5. VIOLATION OF ILLINOIS'S BIOMETRIC INFORMATION PRIVACY ACT, 740 ILCS 14/1, et seq.
- 6. ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESSPRACTICES ACT 815 ILL. COMP STAT. §§ 505, et seq.
- 7. ILLINOIS CONSUMER FRAUD AND DECEPTIVE BUSINESS PRACTICES ACT 815 ILL. COMP. STAT. §§ 510/2, et seq.
- 8. NEGLIGENCE
- 9. INVASION OF PRIVACY
- 10. INTRUSION UPON SECLUSION
- 11. LARCENY/RECEIPT OF STOLEN PROPERTY
- 12. CONVERSION
- 13. UNJUST ENRICHMENT
- 14. FAILURE TO WARN
- 15. NEW YORK GENERAL BUSINESS LAW §§ 349, et seq.

Litigation

A.T. v. OpenAI LP, No. 23-04557 (N.D. Cal. Filed Sept. 5, 2023)

Counsel for Plaintiffs and the Proposed Classes

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

PLAINTIFFS A.T., J.H., individually, and on behalf of all others similarly situated,

Plaintiffs,

vs.

OPENAI LP, OPENAI INCORPORATED, OPENAI GP, LLC, OPENAI STARTUP FUND I, LP, OPENAI STARTUP FUND GP I, LLC, OPENAI STARTUP FUND MANAGEMENT LLC, MICROSOFT CORPORATION and DOES 1 through 20, inclusive,

Defendants.

Case No.:

CLASS ACTION COMPLAINT

1. VIOLATION OF ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. §§ 2510, *et seq.*
2. VIOLATION OF THE COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030
3. VIOLATION OF THE CALIFORNIA INVASION OF PRIVACY ACT ("CIPA"), CAL. PENAL CODE § 631
4. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, BUSINESS AND PROFESSIONS CODE §§ 17200, *et seq.*
5. NEGLIGENCE
6. INVASION OF PRIVACY
7. INTRUSION UPON SECLUSION
8. LARCENY/RECEIPT OF STOLEN PROPERTY
9. CONVERSION
10. UNJUST ENRICHMENT
11. NEW YORK GENERAL BUSINESS LAW §§ 349, *et seq.*

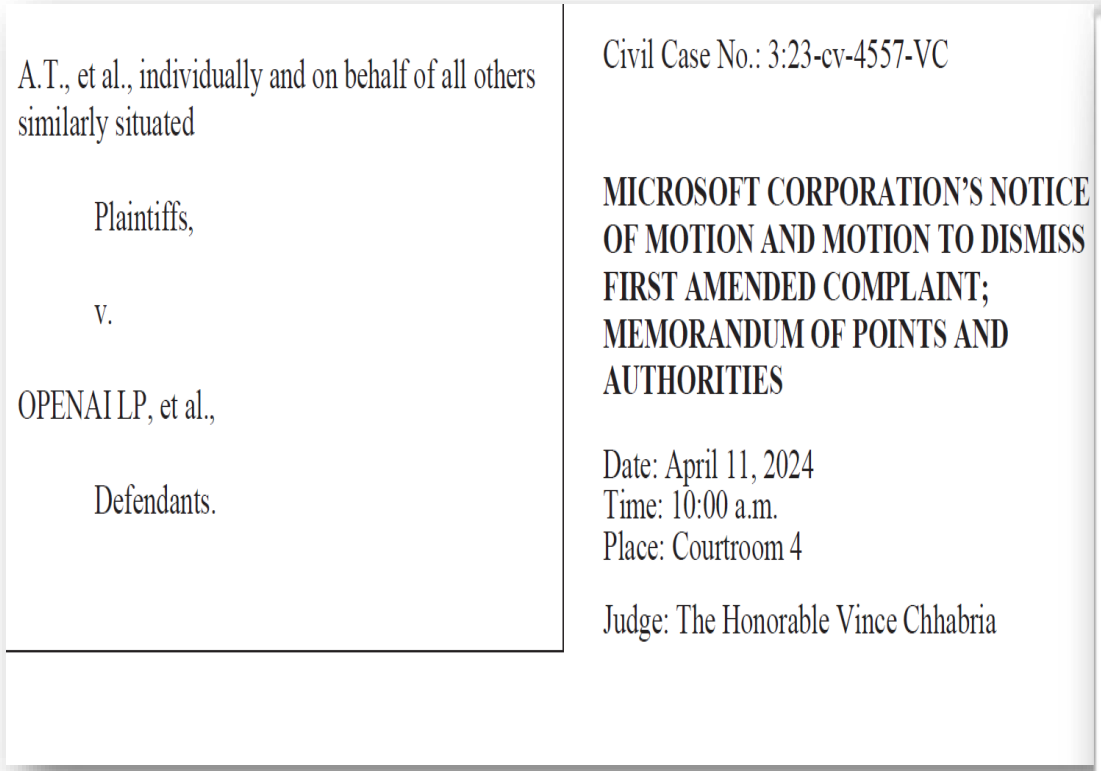
DEMAND FOR JURY TRIAL

"Defendants' disregard for privacy laws is matched only by their disregard for the potentially catastrophic risk to humanity."

"Products only reached the level of sophistication they have today due to training on stolen, misappropriated data, and Defendants continue to misappropriate data, scraping from the internet without any notice or consent, as well as taking personal information from the Products' 100+ million registered users without their full knowledge and consent."

"Compounding this massive invasion of privacy, OpenAI offers no effective procedures at this time for individuals to request for their information/training data to be deleted."

Litigation
A.T. v. OpenAI LP, No. 23-04557 (N.D. Cal. Motion to Dismiss Filed Feb. 8, 2024)



A.T., et al., individually and on behalf of all others similarly situated

Plaintiffs,

v.

OPENAI LP, et al.,

Defendants.

Civil Case No.: 3:23-cv-4557-VC

MICROSOFT CORPORATION'S NOTICE OF MOTION AND MOTION TO DISMISS FIRST AMENDED COMPLAINT; MEMORANDUM OF POINTS AND AUTHORITIES

Date: April 11, 2024
Time: 10:00 a.m.
Place: Courtroom 4

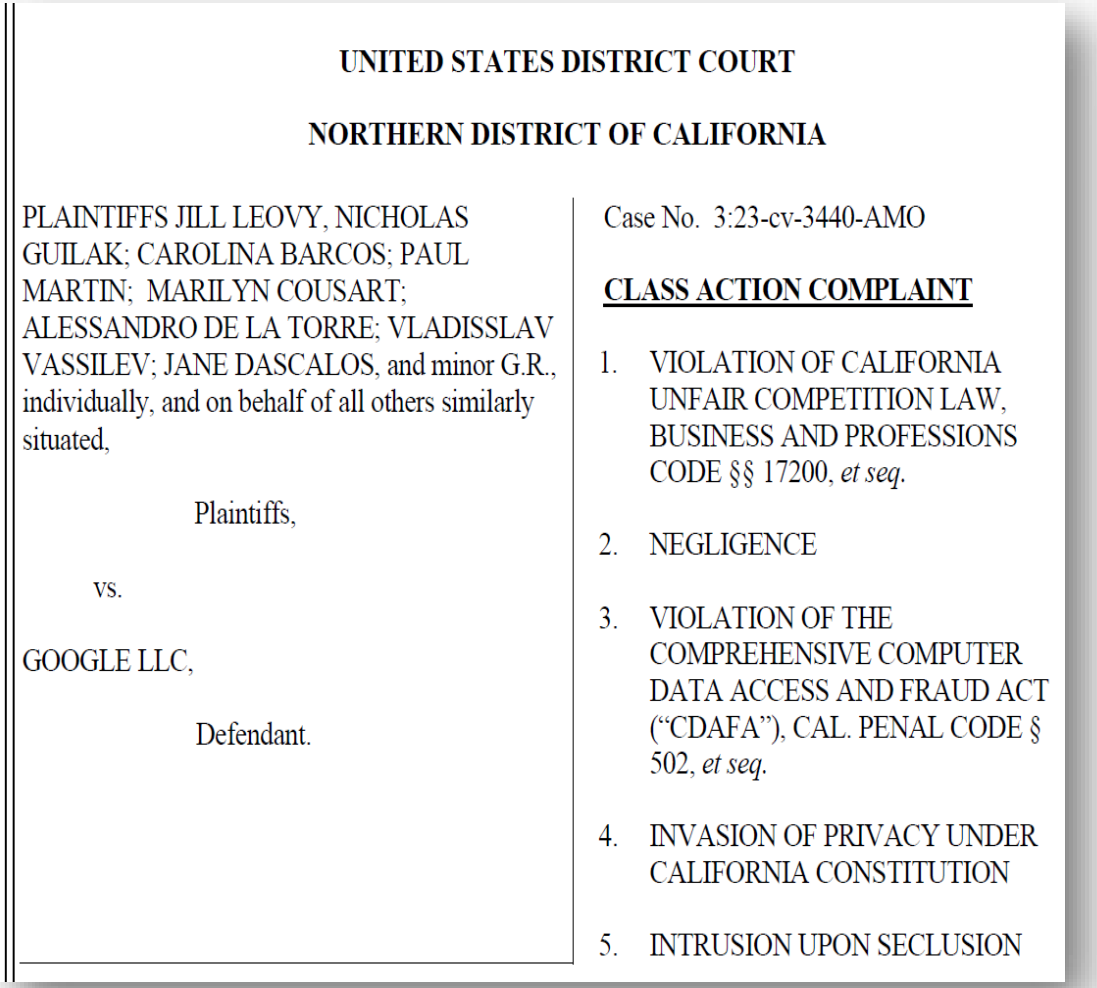
Judge: The Honorable Vince Chhabria

"**Plaintiffs do not plead any facts plausibly showing they have been affected by any of the supposed 'scraping,' 'intercepting,' and 'eavesdropping' they allege**. Nowhere do they say what of their private information Microsoft ever improperly collected or used; nor do they identify any harm they individually suffered from anything that Microsoft allegedly did. Plaintiffs cannot state a claim based on the hypothetical experiences of others."

"Both theories fail because Plaintiffs do not offer any well-pleaded allegations as to how Microsoft performed the alleged interception of communications on non-Microsoft websites or how either Microsoft or OpenAI allegedly intercepted communications with Microsoft services "integrating" ChatGPT…."

Litigation

Leovy v. Google LLC, No. 23-3440 (N.D. Cal. Amended Complaint Filed Jan. 5, 2024)



UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

PLAINTIFFS JILL LEOVY, NICHOLAS GUILAK; CAROLINA BARCOS; PAUL MARTIN; MARILYN COUSART; ALESSANDRO DE LA TORRE; VLADISSLAV VASSILEV; JANE DASCALOS, and minor G.R., individually, and on behalf of all others similarly situated,

Plaintiffs,

vs.

GOOGLE LLC,

Defendant.

Case No. 3:23-cv-3440-AMO

CLASS ACTION COMPLAINT

1. VIOLATION OF CALIFORNIA UNFAIR COMPETITION LAW, BUSINESS AND PROFESSIONS CODE §§ 17200, *et seq.*
2. NEGLIGENCE
3. VIOLATION OF THE COMPREHENSIVE COMPUTER DATA ACCESS AND FRAUD ACT ("CDAFA"), CAL. PENAL CODE § 502, *et seq.*
4. INVASION OF PRIVACY UNDER CALIFORNIA CONSTITUTION
5. INTRUSION UPON SECLUSION

"Plaintiff Barcos never anticipated that her content posted to Instagram, Twitter, TikTok, Snapchat, or Facebook…would be scraped to train AI or otherwise used by a third party like Google in a manner that violates the terms of use of these websites."

"Defendant has scraped websites with confidential financial information…. Defendant has scraped websites with private health information ("PHI")…."

"Given Defendant's ongoing theft and access to Gmail, Google Search, and other data generating sources, this goldmine of data is growing day by day, and with it, the resulting risk to millions of consumers."

"On July 1, 2023, Google quietly amended its privacy policy to openly assert that it scrapes publicly available information from the web to train its AI Products, including "Bard" and "Cloud AI."

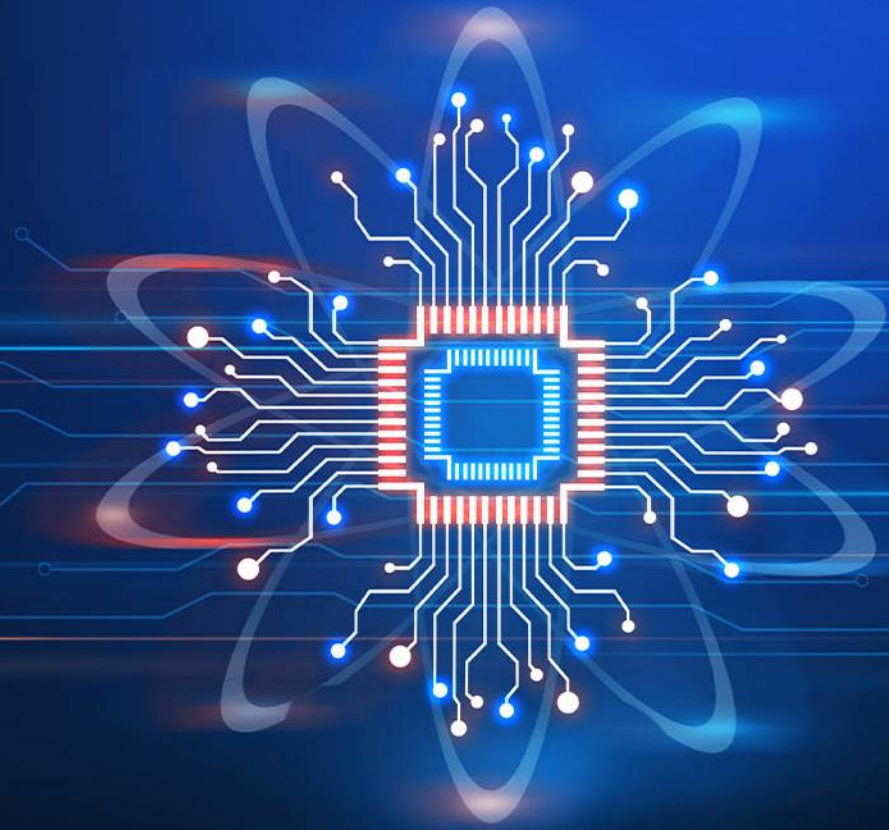
Litigation – Health Data

- Ongoing lawsuits over use of AI to allegedly erroneously deny patient services or to purportedly override physician decisions
  - E.g., *Estate of Gene B. Lokken v. UnitedHealth Group, Inc.*, No. 23-03514 (D. Minn. Filed Nov. 14, 2023)
  - Complaint: “"The nH Predict AI Model saves [UnitedHealth] money by allowing them to deny claims they are obligated to pay and otherwise would have paid by eliminating the labor costs associated with paying doctors and other medical professionals for the time needed to conduct an individualized, manual review of each of its insured's claims.”

Related Litigation:

- *Barrows v. Humana, Inc*., No. 23-00654 (W.D. Ky. Filed Dec. 12, 2023) (putative class action alleging deployed AI in place of human doctors to wrongfully deny elderly patients care owed to them under Medicare)
- *Kisting-Leung v. Cigna Corp*., No. 23-00698 (E.D. Cal. Filed July 24, 2023) (allegations that Cigna developed an algorithm to enable doctors to automatically deny payments in batches of hundreds or thousands at a time for treatments that do not match certain pre-set criteria)

AI & Privacy: EU Update



EU Enforcement Action – ChatGPT Update

…one month later…

European Data Protection Authority Recent Actions:

- Italy – Was banned, then reinstated
- Spain – Investigation
- Germany – Questions raised
- France – Complaints received
- European Data Protection Board – Dedicated task force

Proskauer

EU Enforcement Action

- Italian DPA notifies OpenAI of complaint that it is violating EU's data protection rules
- OpenAI has until the end of the month to respond

ChatGPT: Italy says OpenAI's chatbot breaches data protection rules

29th January 2024, 11:29 EST

Share

By Imran Rahman-Jones
BBC News

Proskauer

Regulating Privacy & AI – The EU Approach – The EU AI Act

- **Timeline**: Political agreement has been reached! Finalized text expected in next few months. In force by 2026 (though some provisions might apply sooner).
- **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**.
- **Overlap with certain EU GDPR** requirements around bias and discrimination, risk assessments and automated decision-making.

EU AI Act – AI Systems

Obligations depend on level of risk

- Unacceptable Risk
- High Risk
- Limited Risk
- Minimal Risk

Penalties: EUR 35 million or 7% of worldwide turnover (higher of)

EU AI Act – General Purpose AI Models

Obligations depend on level of risk

First Tier – All general purpose

Second Tier – “Systemic risk”

Penalties: EUR 15 million or 3% of worldwide turnover (higher of)

AI & Privacy: Other Updates & Approaches

OECD AI Principles

OECD AI Principles - Endorsed by 42 countries:

- **Transparency**
- **Diversity, non-discrimination and fairness**
- **Robustness and safety**
- **Accountability**
- **Societal and environmental well-being**

Global Developments

May 2023 - G7 leaders confirmed the Hiroshima AI Process

June 2023 - EU held an AI stakeholders meeting as part of the US-EU Trade & Tech Council

October 2023 - United Nations announced a new AI advisory board

November 2023 - UK hosted the AI safety summit

UNESCO/the International Organization for Standardization/African Union/Council of Europe

UK & Canada

UK

- “Pro-innovation” & “industry led” approach
- Proposal of targeted binding requirements
- ICO AI Guidance

Canada

- Artificial Intelligence and Data Act (AIDA)
- Voluntary Code of Conduct
- Privacy Commissioner - Principles for responsible, trustworthy and privacy-protective Gen AI technologies

AI Privacy Risk Management Strategies

AI Privacy Risk Management:
Leveraging the Pillars of Your Privacy Governance Program

- Privacy by Design DPIAs
- Transparency
- Process Data Lawfully
- Choices for Data Subjects
- Have Clear Protocols for Sensitive Data (Input & Output)
- Education
- Avoid Inadvertent Discrimination
- De-Identify Data*
- Privacy-Forward Culture

AI Privacy Risk Management

- Create an AI Taskforce
  - Develop and advocate for a comprehensive AI Governance Framework
  - Consider the NIST Artificial Intelligence Risk Management Framework (AI RMF 1.0) (nist.gov) as a foundation
- Create an internal policy for use of Generative AI
  - Prohibit input of personal information
- Leverage technology solutions to reduce risk
  - Differential privacy
  - Federated learning

Business Use of AI – Enterprise AI Tools and Protections

Enterprise privacy at OpenAI

OpenAI debuts ChatGPT subscription aimed at small teams

Comment

Kyle Wiggers @kyle_l_wiggers / 12:00 PM EST • January 10, 2024

Ownership: You own and control your data

- ✓ We do not train on your business data (data from ChatGPT Team, ChatGPT Enterprise, or our API Platform)
- ✓ You own your inputs and outputs (where allowed by law)
- ✓ You control how long your data is retained (ChatGPT Enterprise)

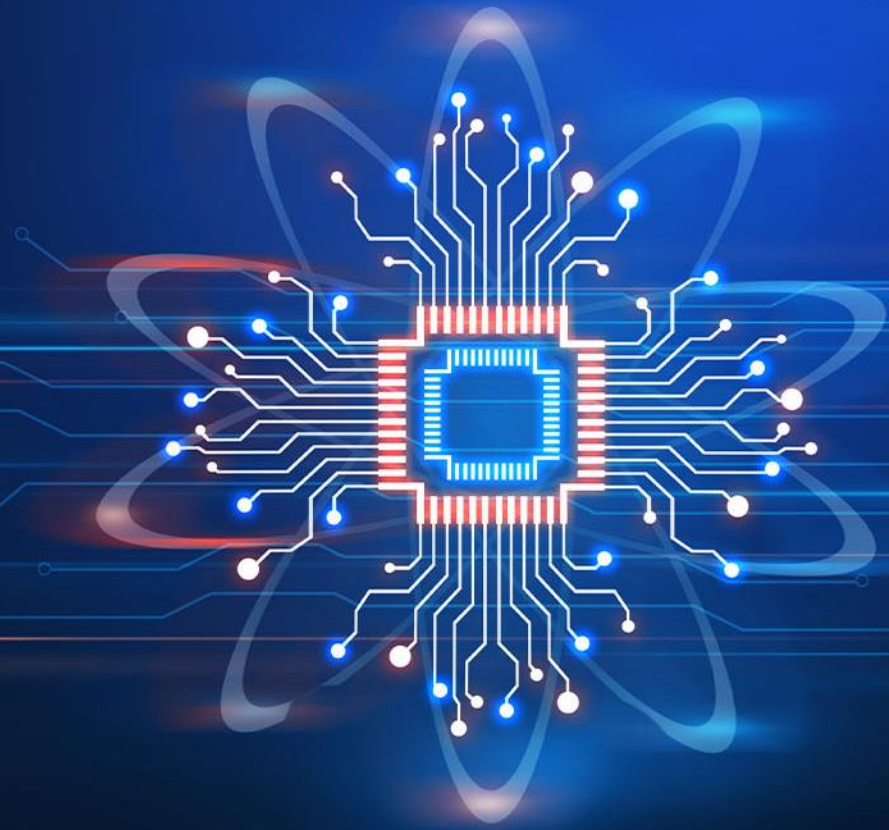
Control: You decide who has access

- ✓ Enterprise-level authentication through SAML SSO (ChatGPT Enterprise and API)
- ✓ Fine-grained control over access and available features
- ✓ Custom models are yours alone to use and are not shared with anyone else

Security: Comprehensive compliance

- ✓ We've been audited for SOC 2 compliance (ChatGPT Enterprise and API)
- ✓ Data encryption at rest (AES-256) and in transit (TLS 1.2+)
- ✓ Visit our Trust Portal to understand more about our security measures

AI & Cybersecurity



AI: Deepfakes and Other Dangers in the News

TECHNOLOGY

A mysterious phone call cloned Biden's voice. Can the next one be stopped?

Regulators struggle to clamp down on deepfakes ahead of the 2024 election.

President Joe Biden speaks in Superior, Wisconsin. | Alex Brandon/AP

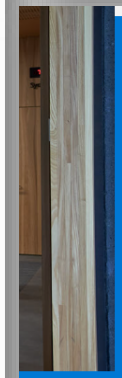
By CHRISTINE MUI
01/29/2024 06:44 PM EST

Happy Valentine's Day! Romantic AI Chatbots Don't Have Your Privacy at Heart

By Jen Caltrider, Misha Rykov and Zoë MacDonald | Feb. 14, 2024

No, Biden Isn't Dead: AI Content Farms Are Here, and They're Pumping Out Fake Stories

A new report found 49 different websites secretly using AI to churn out low-quality posts and rake in advertising revenue.



Research Threat intelligence Microsoft Copilot for Security
Threat actors

12 min read

Staying ahead of threat actors in the age of AI

By Microsoft Threat Intelligence

Taylor Swift, the pope, Putin: in the age of AI and deepfakes, who do you trust?

Rumours and gossip changed the course of French history. Now they're weapons for 'newsfluencers' and dictators in the 21st-century information wars

Generative AI financial scammers are getting very good at duping work email

PUBLISHED WED, FEB 14 2024•11:54 AM EST | UPDATED FRI, FEB 16 2024•1:51 PM EST

Ellen Sheng
@ELLENSHENG

SHARE

AI tools such as ChatGPT are generating a mammoth increase in malicious phishing emails

PUBLISHED TUE, NOV 28 2023•10:39 AM EST

Proskauer

AI as a foe to Cybersecurity: Generative AI Can Be Used to Create Fake Content and Assist in Financial and Cyber Crime

Deepfake videos/robocalls and imposer scams; election tampering

Voice clones

Pump and dump schemes; stock manipulation

Fake websites/content

Fake social media profiles and posts, consumer reviews

"Karma farming"

(Creating spammy content to populate fake social media accounts to get likes and views to give them an air of authenticity)

Assist in creating code for malware, ransomware, phishing scams, injection attacks, and attacks from known foreign state hackers

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

UK's National Cyber Security Centre:

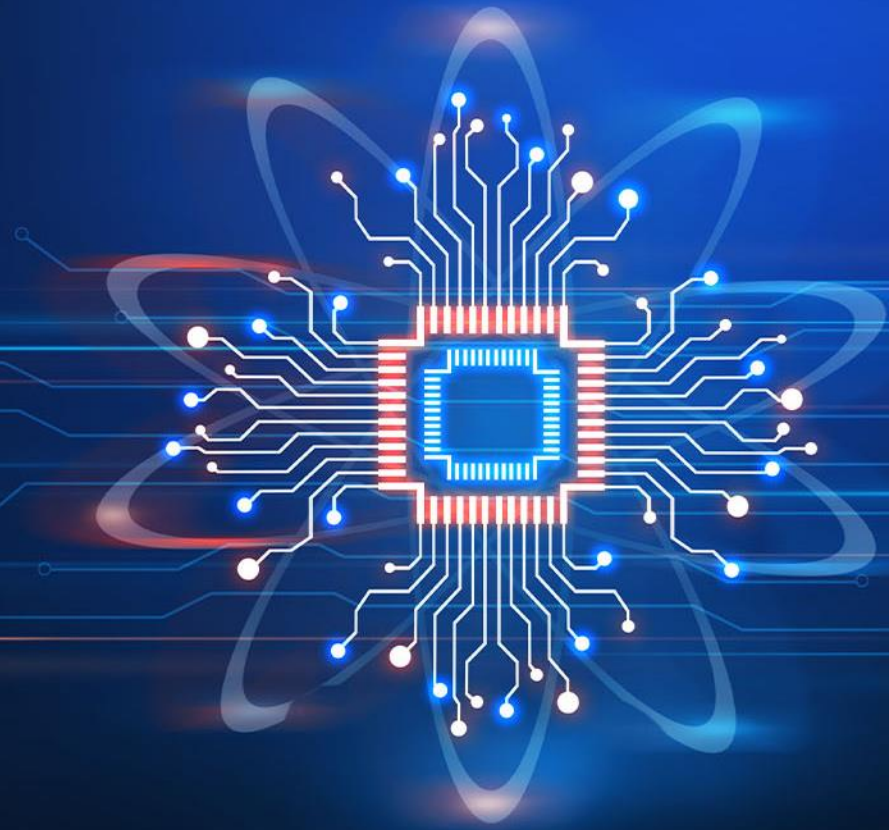
- "*more state and non-state actors* [will] *obtain capabilities and intelligence not previously available to them*" which "*will have a profound impact on the threat landscape*"
- "*Cyber resilience challenges will become more acute as the technology develops*"

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

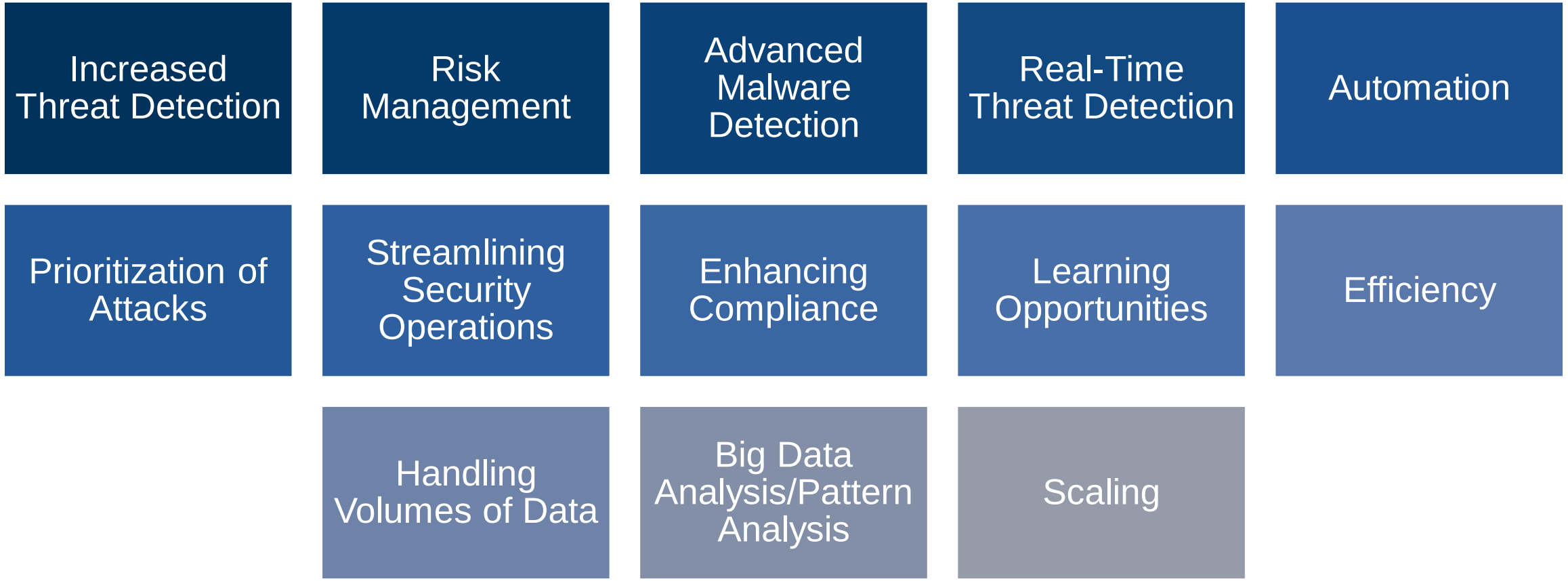
- "*Generative AI ushers in a world of new risks and threats*"
- "*Trustworthy GenAI is not possible without secure data*"
- Advises leaders to:
  - Understand AI exposure
  - Secure AI pipeline
  - Invest in new defences

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

A Silver Lining?



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*"

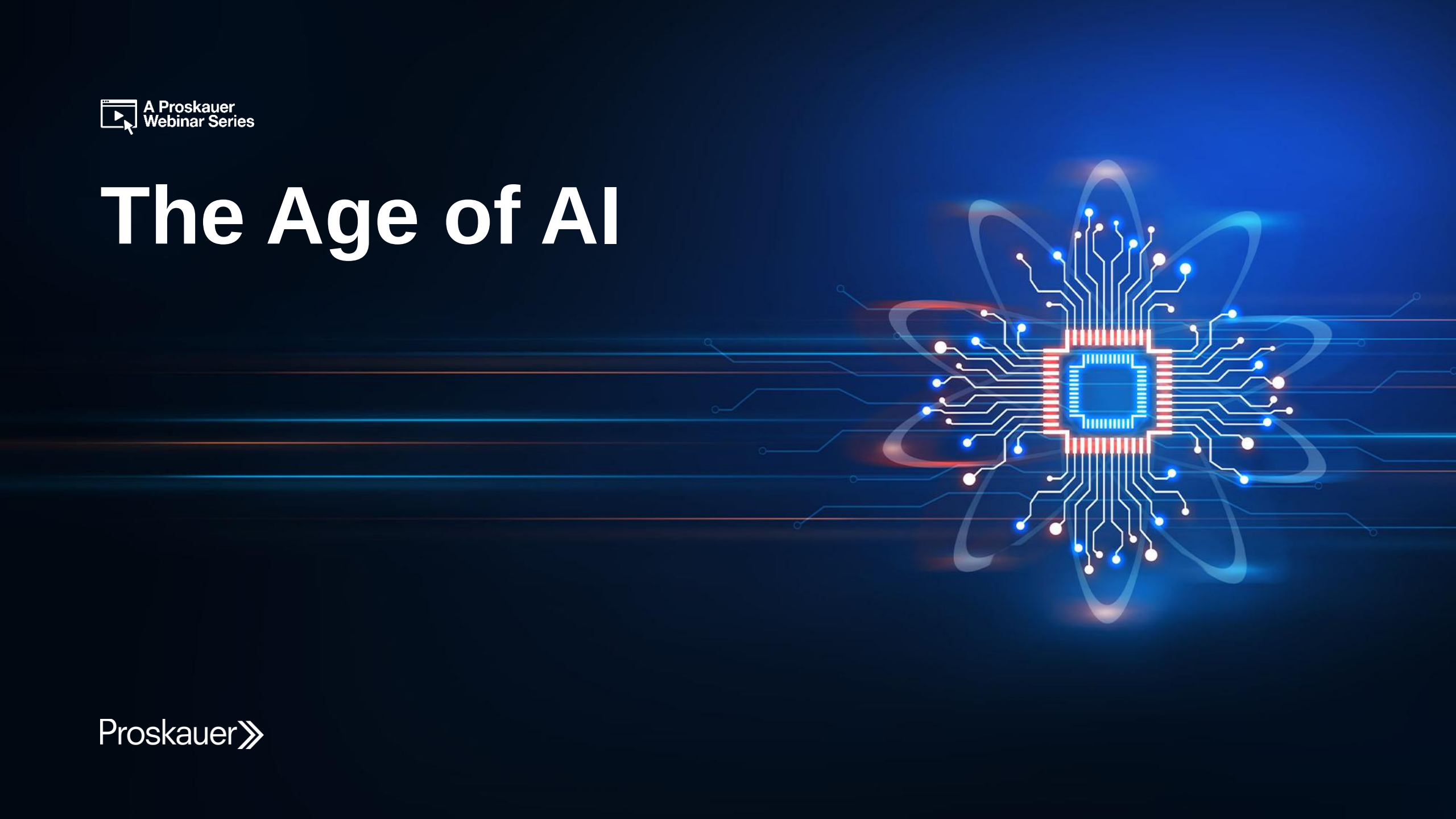
AI as a Friend to Privacy: Privacy Operations

- Data mapping & classification
  - Sensitive Data (+automated protection)
- Data inventories / Records of Processing
- Data Protection Impact Assessments
- Data Subject requests
  - Unstructured data eDiscovery (e.g., employee requests)
  - Actioning requests across data ecosystem
- Vendor risk assessments
- Data breach notifications
- Training & testing exercises

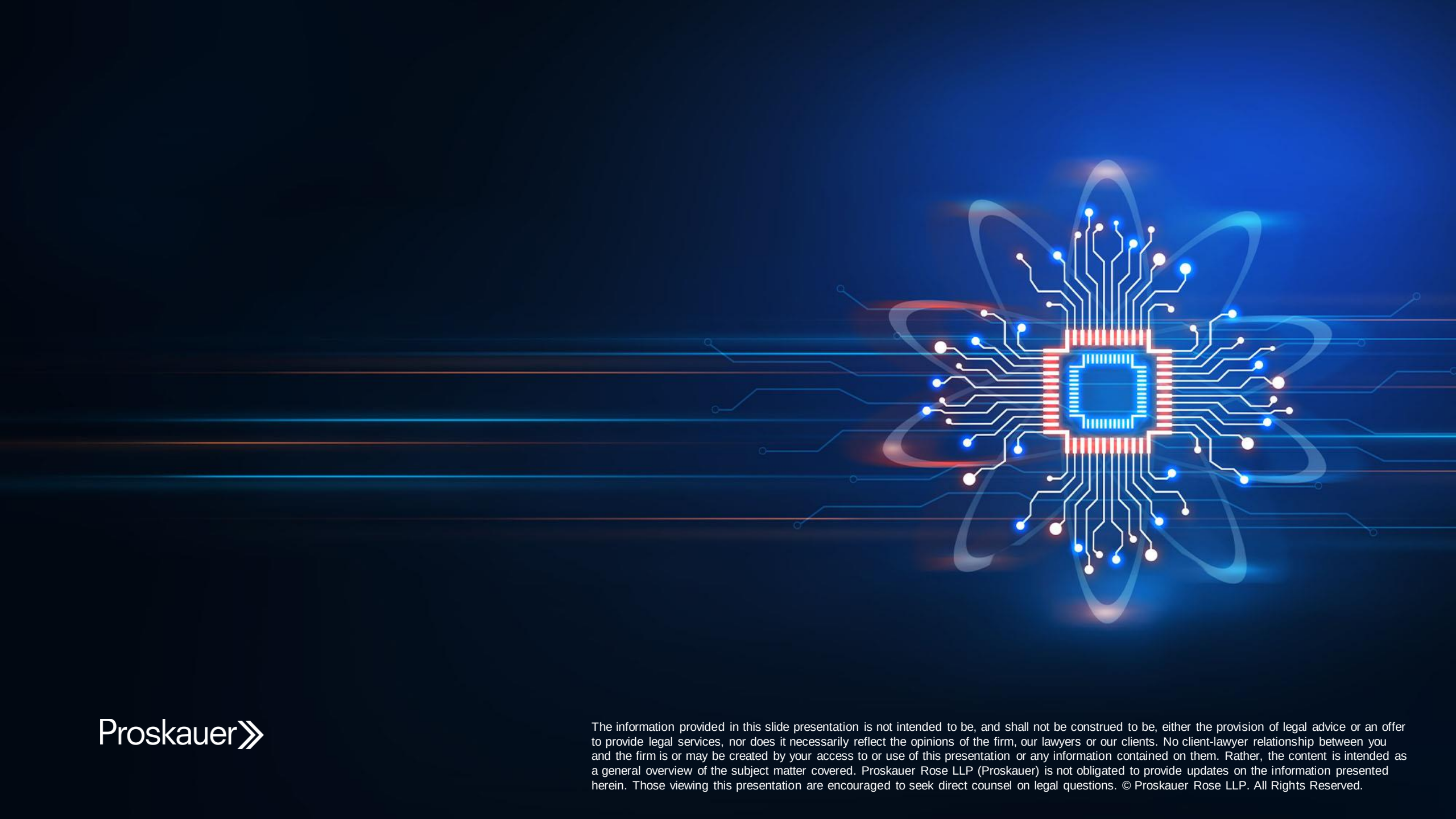
Proskauer

A Proskauer Webinar Series

The Age of AI



Proskauer



Proskauer