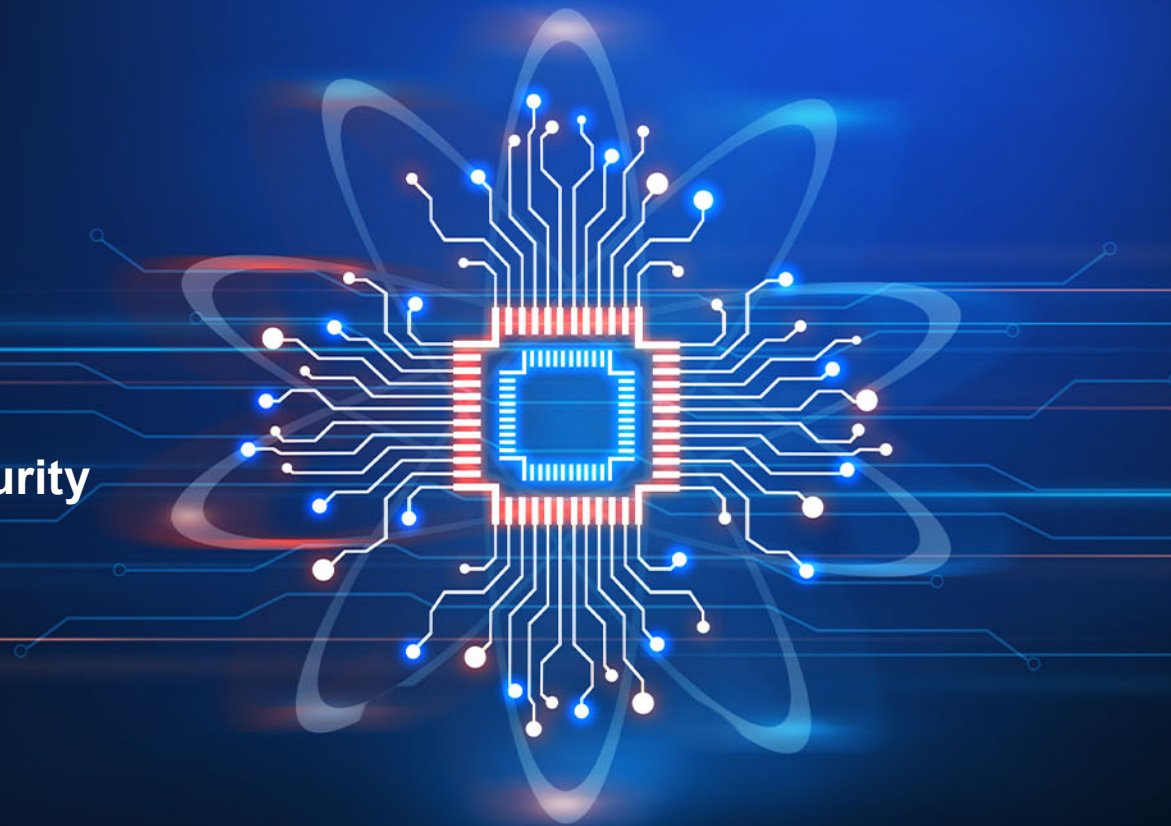


# The Age of AI - Privacy & Data Security

**Ryan P. Blaney, Partner, Head of Privacy & Cybersecurity**  
**Kelly McMullon, Special Counsel**

May 2, 2023



# Agenda

## Introduction

---

## European Developments

- GDPR & AI
  - Chat GPT and the approach of Regulators in the EU
- 

## US Developments

- Legal landscape for Privacy & AI
  - FTC Developments
  - Case Study: Healthcare
- 

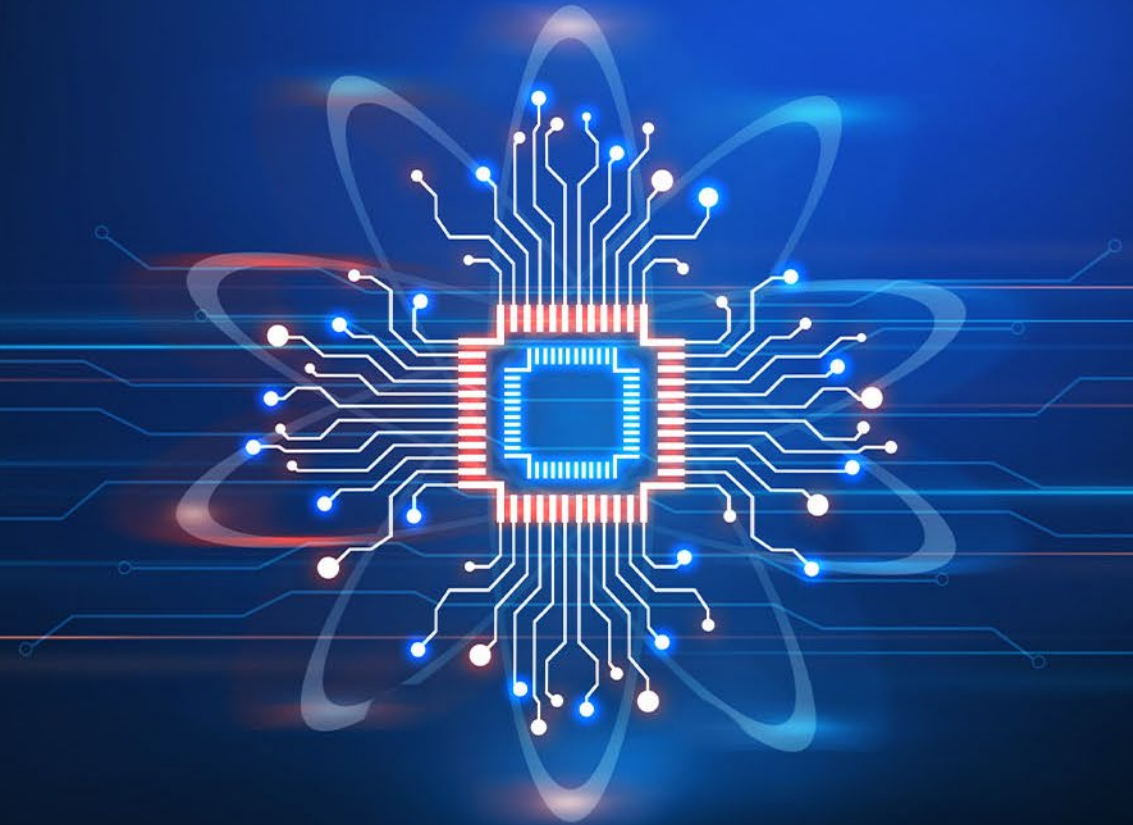
## Privacy & Ethical Considerations

---

## Cybersecurity Considerations

---

# Introduction to AI





# GPT-4 Response on What is Generative AI?

R What is generative AI



Generative AI refers to a type of artificial intelligence that is designed to generate new content or data. This can include everything from text to images to audio and beyond. Generative AI algorithms are trained on large datasets and use statistical methods to learn patterns in the data. Once trained, they can then generate new content that is similar in style or structure to the original data.



One popular example of generative AI is the language model GPT-3, which is capable of generating human-like text based on a given prompt. Another example is the deep learning algorithm called StyleGAN, which can generate realistic images of faces that do not exist in reality.

Generative AI has a wide range of potential applications, from creating new art and music to generating realistic simulations for scientific research. However, it also raises ethical and societal concerns, such as the potential for misuse in the creation of deepfakes or the potential to automate jobs traditionally done by humans.

# Introduction to AI: AI and GI

---

## AI:

Computer systems that perform tasks requiring human-like cognition, enabling machines to autonomously learn, reason, and adapt through experience.

## GAI:

A subset of AI focused on creating new, original content or data, such as images, text, or music, by autonomously learning patterns and features from existing datasets.

# Introduction to AI: Large Language Model

## Large Language Model

An AI system designed to understand and generate human-like text by learning from vast amounts of textual data

It is trained in two steps:

**pre-training** on vast datasets to learn grammar and facts and to predict the next word in a sentence by analysing massive datasets containing diverse text sources.

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





# ChatGPT: Sign-In

**ChatGPT**

---

**How we collect data**

-  Conversations may be reviewed by our AI trainers to improve our systems.
-  Please don't share any sensitive information in your conversations.

[Back](#) [Next](#)



# GPT-4 Response Regarding Privacy Concerns

**R** what are the privacy concerns with generative AI?



Generative AI, which includes algorithms such as Generative Adversarial Networks (GANs) and Variational Autoencoders (VAEs), has raised various privacy concerns. Here are some examples:



1. **Data Privacy:** Generative AI models typically require large amounts of data to be trained, and this data often contains sensitive information. There is a risk that personal information can be leaked if the data used to train these models is not adequately anonymized or secured. Additionally, once a generative AI model is trained, it may be able to generate synthetic data that is similar to the original data, which can also pose a privacy risk.
2. **Biased Data:** Another concern is that generative AI models may perpetuate and even amplify existing biases in the data used to train them. For example, if a generative AI model is trained on data that is biased against certain groups of people, the model may generate synthetic data that is also biased.
3. **Deepfakes:** Generative AI can be used to create deepfake videos and images that can be used to spread disinformation or manipulate public opinion. This poses a significant threat to privacy and can have serious consequences for individuals and society as a whole.
4. **Adversarial Attacks:** Generative AI models can be vulnerable to adversarial attacks, where an attacker intentionally feeds the model data designed to cause it to produce a specific output. This can be used to exploit vulnerabilities and potentially use the privacy of individuals or

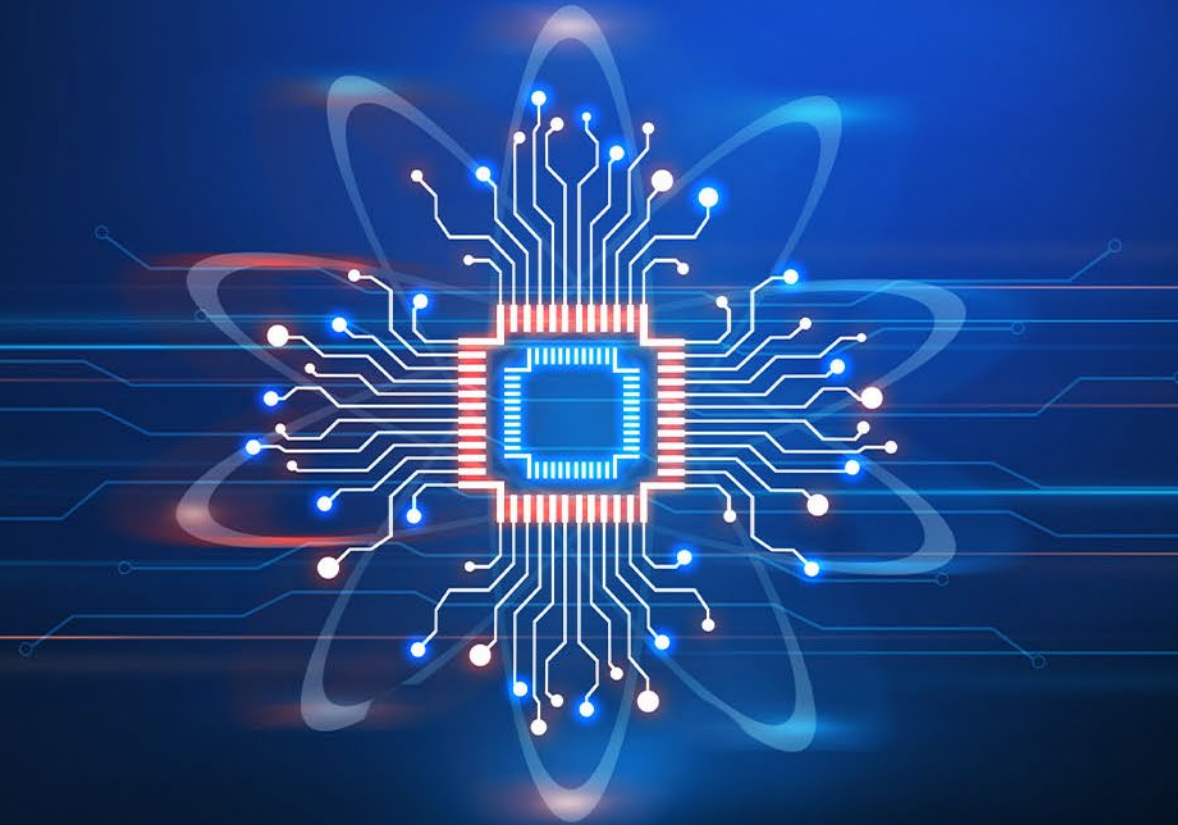
↻ Regenerate response

Send a message.





# European Developments



# ChatGPT - European Data Protection Authority Recent Actions

- **Italy** – Was banned
- **Spain** – Investigation
- **Germany** – Questions raised
- **France** – Complaints received
- **EDPB** – Dedicated task force
- **UK** – A different approach?

FROM POLITICO PRO

## ChatGPT is entering a world of regulatory pain in Europe

AI chatbot makes itself an easy target for privacy regulators as fears around artificial intelligence grow.



# Italian DPA Actions

- **Mar. 2023:** Italian DPA, il Garante, issued a temporary limitation on the processing of Italian users' data by OpenAI, citing a March 20 data breach (misconfiguration in cache system) affecting ChatGPT user conversations and payments and a lack of age verification re: children under 13.
  - “[N]o information is provided to users and data subjects whose data are collected by Open AI....”
  - “[T]here appears to be no legal basis underpinning the massive collection and processing of personal data in order to ‘train’ the algorithms on which the platform relies.”
  - “[I]nformation made available by ChatGPT does not always match factual circumstances, so that inaccurate personal data are processed.”
- **Apr. 2023:** In response, OpenAI geoblocked Italian users (which reportedly can be circumvented with a VPN).

## Italy became the first Western country to ban ChatGPT. Here's what other countries are doing

PUBLISHED TUE, APR 4 2023 4:48 AM EDT | UPDATED MON, APR 17 2023 1:24 AM EDT

 Ryan Browne  
@RYAN\_BROWNE\_

SHARE [f](#) [t](#) [in](#) [✉](#)

### KEY POINTS

- Italy last week became the first Western country to ban ChatGPT, the popular AI chatbot.

## OpenAI geoblocks ChatGPT in Italy

Natasha Lomas @riptari / 6:15 AM EDT • April 1, 2023

# Italian DPA Actions

Italian DPA set April 30<sup>th</sup> deadline to comply with its recommendations – Ban now lifted:

1. OpenAI will have to draft and make available, on its website, an information notice describing the arrangements and logic of the data processing required for the operation of ChatGPT along with the rights afforded to data subjects.
2. Age gate filtering out of underage users.
3. Legal basis of the processing of users' personal data for training algorithms – DPA ordered OpenAI to rely – in line with the accountability principle – on either consent or legitimate interest as the applicable legal basis.
4. Tools for non-users and users to exercise rights to object to the processing of their personal data as relied upon for the operation of the algorithms.

## ChatGPT: Italian SA to lift temporary limitation if OpenAI implements measures

### 30 April set as deadline for compliance

OpenAI will have to comply by 30 April with the measures set out by the Italian SA concerning transparency, the right of data subjects – including users and non-users –, and the legal basis of the processing for algorithmic training relying on users' data. Only in that case will the Italian SA lift its order that placed a temporary limitation on the processing of Italian users' data, there being no longer the urgency underpinning the order, so that ChatGPT will be available once again from Italy.

Therefore, several concrete measures will have to be implemented by the company in accordance with today's decision by the SA.



## ITALY

### Garante Authorises OpenAI to Reinstate ChatGPT

Based on the actions taken by OpenAI, including expanded information provided to EU users and non-users, the Garante authorised the reinstatement of ChatGPT for Italian users.

# Efforts to Comply

- In this “incognito” mode, chat history is disabled and will not be used to train the AI models (though new chats are saved for 30 days and reviewed, if necessary, to monitor for abuse, and then deleted).
- Settings will also make it easier to export user data and add transparency to what data OpenAI is collecting.
- ChatGPT Business, a paid service – user prompts will not be used to train the AI.

## OpenAI adds a more private option to ChatGPT

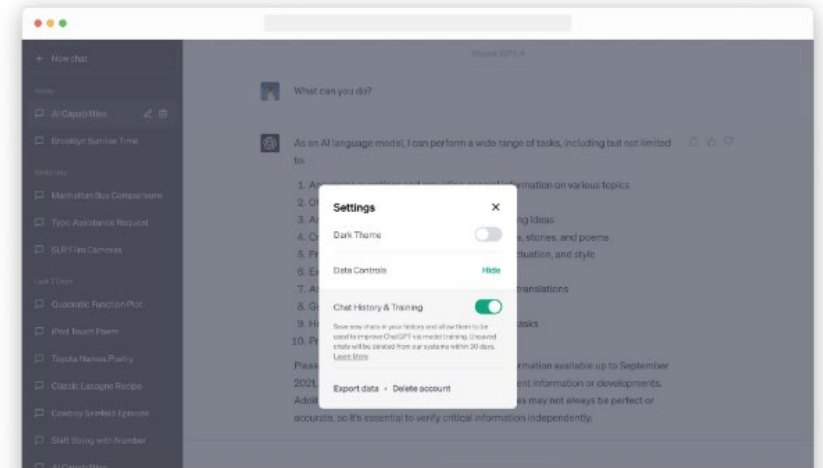
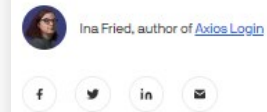


Image: OpenAI

# Key GDPR Considerations

---

Lawfulness, Fairness  
and Transparency

Controller/Joint  
Controller/Processor

Data Protection  
Impact Assessments

Security

Purpose Limitation

Data Minimisation

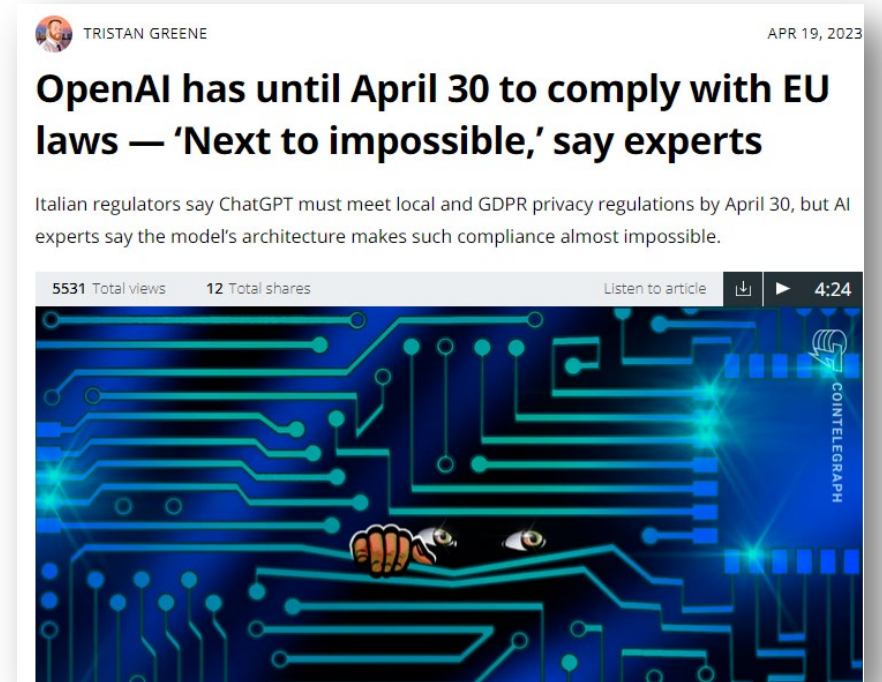
Accuracy

Rights Requests

Automated Decision-  
Making

# Efforts to Comply

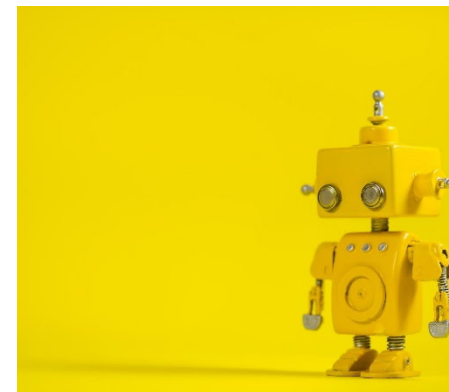
- Still, there are some open questions re: how to reach full compliance with the GDPR?
  - **“Black box” issue:** Developers may not know the precise extent of what’s in a dataset, and because machine learning involving multiple data points to create an output, it’s likely not possible to know if a piece of personal data was collected and used to process a particular output.
  - **Consents:** Can an AI developer, like OpenAI, prove that its prior collection of certain website data for AI training was done with proper user consents or else prove it had a “legitimate interest”? Similar concerns with using user prompts to train AI (though that issue was perhaps resolved by OpenAI’s incognito mode offering).
  - **Data rights:** How does a data subject employ their rights under the GDPR with respect to data that may be in a large language model dataset (even if such data could be identified, could one person’s “data” even be removed from an AI training dataset? Is “machine unlearning” possible?)



# Not just Data Protection but the AI Act

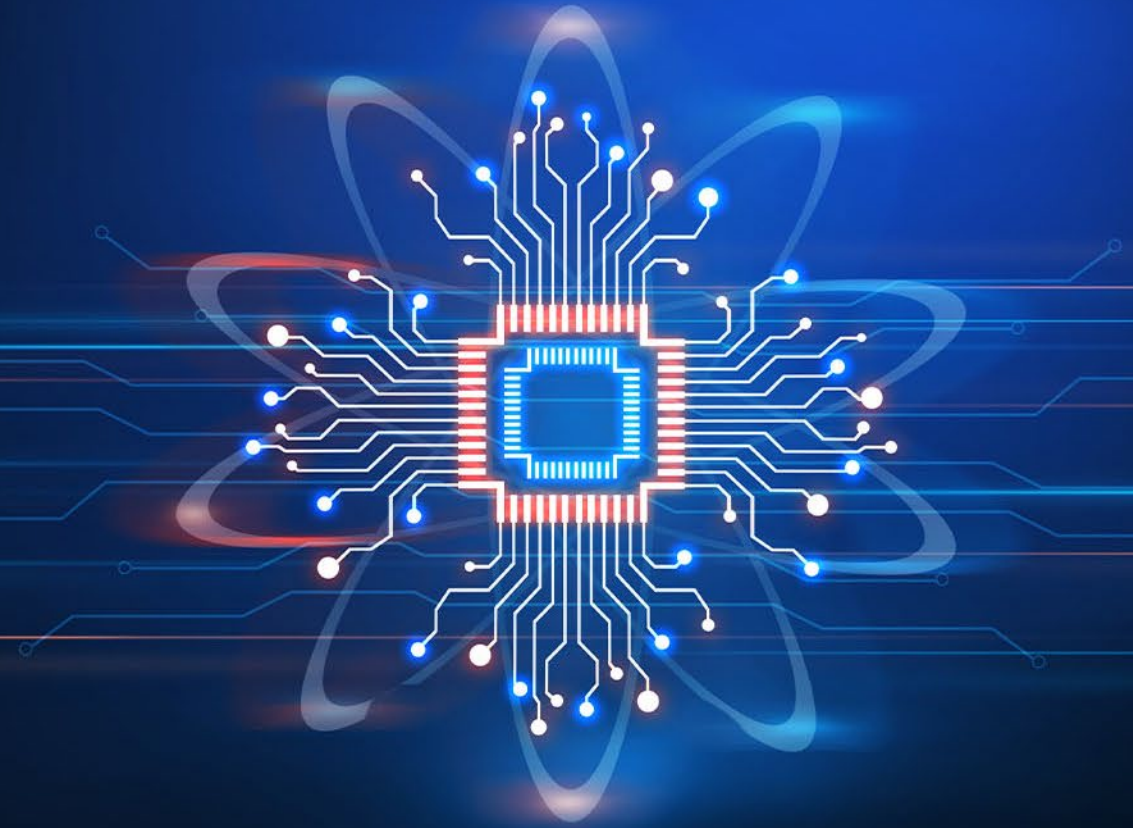
---

- EU AI Regulation
- Risk-based approach to regulating AI applications - minimal to high and unacceptable risks)
- High risk AI systems will be subject to strict obligations before they go to market, including adequate risk assessments and traceability requirements.
- Key Question - Will generative AI applications be considered high-risk?





# US Developments



# US Developments - Legal landscape for Privacy & AI

- While the EU is working toward an AI regulation, 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:** Efforts in Senate to establish rules on AI.
- **White House Blueprint for an AI Bill of Rights:** Outlines five principles – safe and effective systems; algorithmic discrimination protections; notice and explanation; and human alternatives to AI systems; and data privacy (“You should be protected from abusive data practices via built-in protections and you should have agency over how data about you is used”).
- **State laws:** Some state laws regarding use of AI in any employment decisions. [covered more in depth in our prior Webinar in this series]
  - Other bills that seek to regulate AI and automated decision-making and require impact assessments for AI tools being debated in state legislatures (e.g., California AB-331)

## Schumer calls for AI rules as ChatGPT surges in popularity

The Senate majority leader has circulated a plan to establish rules on AI to address national security concerns as ChatGPT becomes the fastest-growing consumer application in history.



## BLUEPRINT FOR AN AI BILL OF RIGHTS

MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE

 OSTP

# Indiana Becomes “Lucky #7” with a Comprehensive Privacy Law

---

- California
  - Colorado
  - Connecticut
  - Utah
  - Virginia
  - Iowa
  - Indiana
- Also, Washington enacted a “consumer health” information privacy law with a private right of action.



# Potential State Level Issues

---



- Original CCPA was silent on automated decision-making.
- However, the CPRA amendments, as well as other state data privacy laws (e.g., Colorado and Connecticut) gives certain rights to consumers re: automated decision-making technology.
- Notably, in March 2023, the CPPA requested pre-rulemaking comments in helping it craft regulations on automated decision-making), including questions about whether access and opt-out rights with respect to automated decision-making should depend on the industry, the technology used, and the sensitivity of the PII.
- In the recently-released Colorado privacy regs, there are rules on opt-out rights of decisions based on automated processing that produce legal or other significant effects on a consumer.

## IN THE MATTER OF OPEN AI (FTC 2023)

*The Federal Trade Commission should open an investigation and order OpenAI to halt the release of GPT models until necessary safeguards are established. These safeguards should be based on the guidance for AI products the FTC has previously established and the emerging norms for the governance of AI.*

- **Mar. 2023:** Center for AI and Digital Policy files a 46-page complaint with the FTC asking it to investigate OpenAI, enjoin further commercial releases of GPT-4, and ensure the establishment of necessary guardrails to protect consumers, businesses, and the commercial marketplace.

# FTC Joint Statement on AI

---

## FTC Chair Khan and Officials from DOJ, CFPB and EEOC Release Joint Statement on AI

April 25, 2023



- “Existing legal authorities apply to the use of automated systems and innovative new technologies just as they apply to other practices.”
- “The FTC are among the federal agencies responsible for enforcing civil rights, non-discrimination, fair competition, consumer protection, and other vitally important legal protections.”
- “Many automated systems rely on vast amounts of data to find patterns or correlations, and then apply those patterns to new data to perform tasks or make recommendations and predictions. While these tools can be useful, they also have the potential to produce outcomes that result in **unlawful discrimination.**”
  - Potential discrimination can come from different sources.
  - Examples: Unrepresented or imbalanced datasets; “black box” and opacity issues; AI designs that do not account for private or public usage;



# Prior FTC Enforcements: “Algorithmic Justice”

---

- *In re Kogan and Nix*, Nos. 182 3016 (Agreement Dec. 18, 2019) (former app developer that with Cambridge Analytics and its former CEO enabled app to collect Facebook data from users and friends; among other things, settlement required defendants to **delete or destroy any personal information collected from consumers via the app and any related work product that originated from the data**).
- *In re Everalbum, Inc.*, No. C-4743 (Decision and Order May 6, 2021) (photo app developer settled FTC allegations that it deceived consumers about its use of facial recognition technology and its retention of the photos and videos of users who deactivated their accounts; as part of the proposed settlement, Everalbum must, among other things, **delete models and algorithms it developed by using the photos and videos uploaded by its users**)
- *U.S. v. Kurbo Inc.*, No. 22-00946 (N.D. Cal. Stipulated Order Mar. 3, 2022) (settlement order requires WW International and Kurbo to delete personal information illegally collected from children under 13 and **destroy any algorithms derived from the data**)

## Questions:

- How relevant are these prior algorithmic-related enforcement actions relevant in the AI arena?
- How worried should a company using a third party’s AI application to process data or develop applications or products about possible enforcement and “algorithmic destruction” remedies from the FTC?

# Case Study – Generative AI & Healthcare

## Generative AI potential uses in healthcare

- Assistance with coding and billing and administrative tasks
- Producing routine insurance/benefits notices or forms
- Integrate generative AI into EHR software to enhance natural language queries and data analysis and spot trends in medical records (in the aggregate).

Could cancer be diagnosed from the sound of a voice?



A \$14 million research project is getting underway in the US to



# Case Study – Generative AI & Healthcare

---



## Potential Risks

- Automation bias and potential discrimination against patients based on race, gender, etc.
- Producing misleading, inaccurate or correct-sounding (but incorrect) output
- Not yet suitable for diagnostic or medical treatment suggestions
- Data security: Concern over additional sensitive medical records and possible sharing/transmittal of patient data or data being used to train AI system
- Privacy: Concern about how new AI-powered systems will use patient data

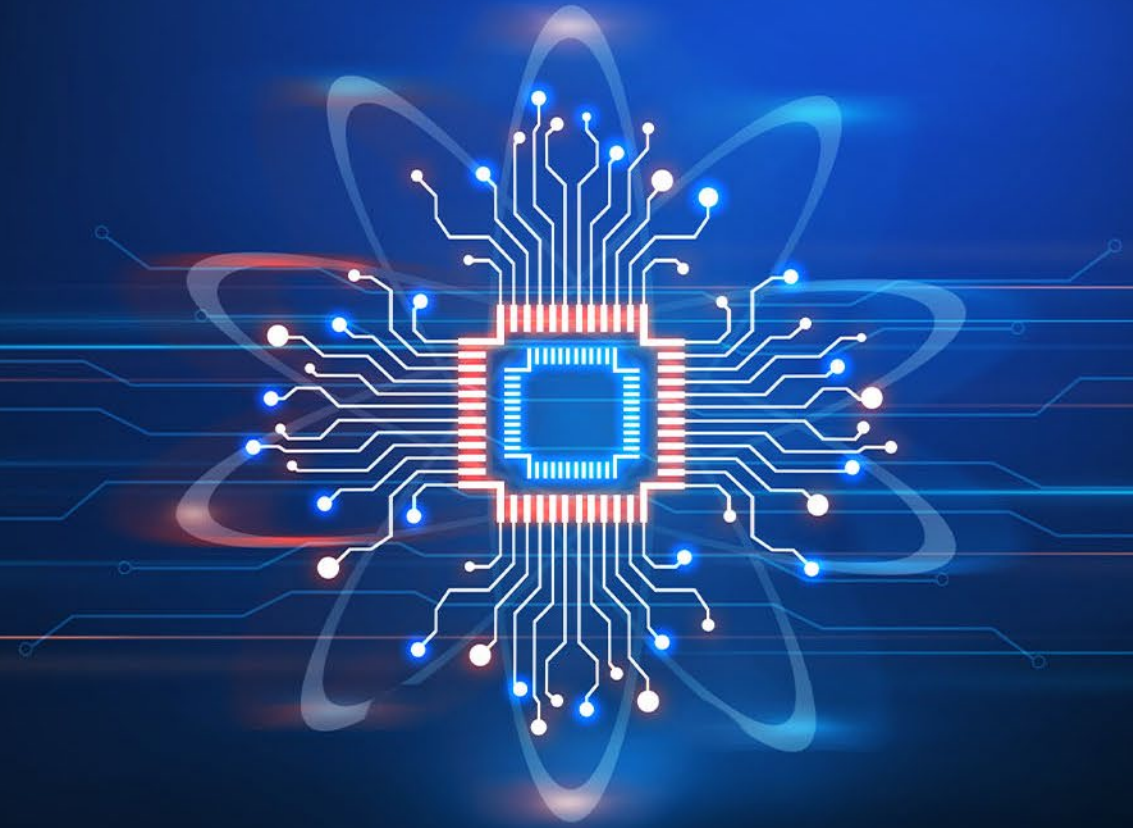
# Some Final US Privacy Questions to Consider

---



- How transparent does a company have to be regarding its use of generative AI applications when it comes to processing consumer data?
- Are there more privacy compliance concerns re: AI automated decision-making in products or services?
- Should every company that intends to use generative AI and related technologies update an existing privacy program to meet the privacy questions of AI?
- Should a company monitor internal use of generative AI (mapping its uses and cataloguing them) to prepare for privacy issues or potential compliance issues in the future (e.g., knowing the extent and types of business uses)?

# Ethical Considerations



# Overarching Privacy, Ethical and Social Responsibility Concerns

- **ESG Commitments**
- **OECD AI Principles**
- **White House Blueprint for an AI Bill of Rights**
- **NIST Trustworthy & Responsible Artificial Intelligence Resource Center:** Voluntary guidance to improve the ability to incorporate trustworthiness considerations into the design, development, use and evaluation of AI products, services and systems.
- **European Convention on Human Rights (ECHR):** Article 8 protects your right to respect for your private life, your family life, your home and your correspondence.



# Overarching Privacy, Ethical and Social Responsibility Concerns

- Discrimination/Bias
- Engendering Trust
- Protecting Public Safety or the Safety of Oneself
- ESG Commitments
- Transparency

## AI 'godfather' Geoffrey Hinton warns of dangers as he quits Google

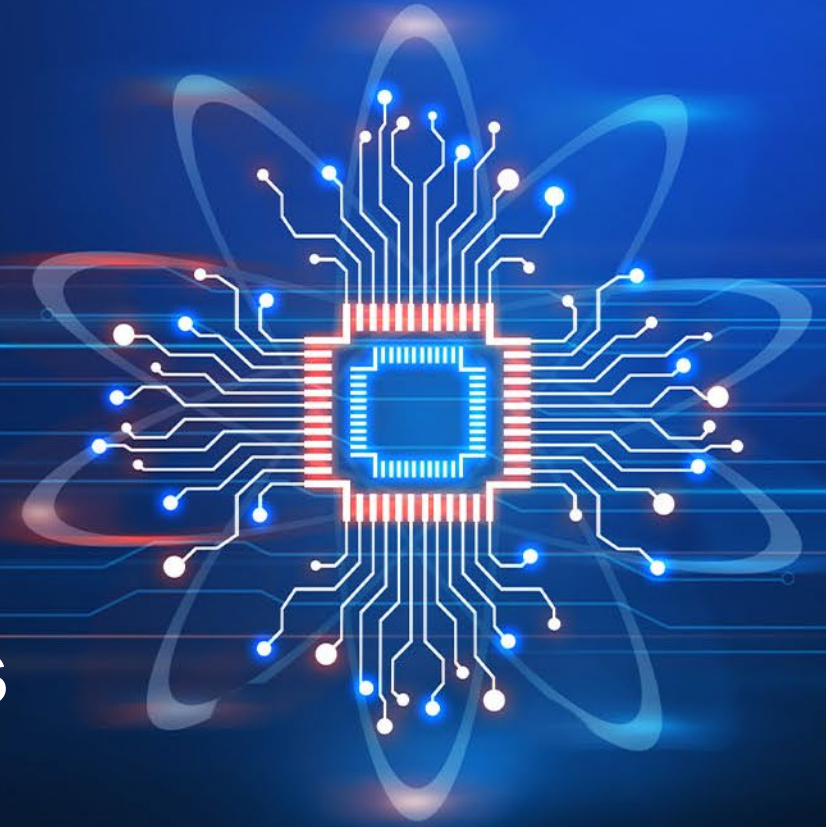
🕒 3 hours ago · 💬 Comments



### *Elon Musk and Others Call for Pause on A.I., Citing 'Profound Risks to Society'*

More than 1,000 tech leaders, researchers and others signed an open letter urging a moratorium on the development of the most powerful artificial intelligence systems.

# Cybersecurity Considerations



# Cybersecurity Considerations

- Cybersecurity concerns “WHEN” OpenAI or similar provider are breached.
- Chat histories and usage and inputted information (which may be sensitive) could be released or used by an attacker for phishing, corporate espionage (particularly if sensitive business information was entered into the prompt).

**BREAKING**

## Samsung Bans ChatGPT Among Employees After Sensitive Code Leak

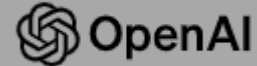
Siladitya Ray Forbes Staff  
*Covering breaking news and tech policy stories at Forbes.*

[Follow](#)

May 2, 2023, 07:17am EDT

# March 20 ChatGPT outage: Here's what happened

An update on our findings, the actions we've taken, and technical details of the bug.



“We took ChatGPT offline earlier this week due to a bug in an open-source library which allowed some users to see titles from another active user’s chat history. It’s also possible that the first message of a newly-created conversation was visible in someone else’s chat history if both users were active around the same time.

The bug is now patched. We were able to restore both the ChatGPT service and, later, its chat history feature, with the exception of a few hours of history.”

# The Hacking of ChatGPT Is Just Getting Started

Security researchers are jailbreaking large language models to get around safety rules. Things could get much worse.

March 31, 2023 - 6 minute read

## Prompt Injection Attack on GPT-4

Product Updates

ILLUSTRATION: JACQUI VANLIEW

IT TOOK ALEX Polyakov just a couple of hours to break GPT-4. When OpenAI released the latest version of its text-generating chatbot in March, Polyakov sat down in front of his keyboard and started entering prompts designed to bypass OpenAI's safety systems. Soon, the CEO of security firm Adversa AI had GPT-4 spouting homophobic statements, creating phishing emails, and supporting violence.



# Generative AI Can Speed the Creation of Fake Content and Assist in Financial and Cybercrime

---

Deepfake videos and imposter scams

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)

AI Hallucinations (false facts)

Assist in creating malware, ransomware, phishing scams, injection attacks

With the emergence of generative AI, it's time to reexamine privacy programs and tabletop exercises to prepare for response to deepfake-like attacks

# Voice Authentications, Avatars, and Data Breach

## Your AI Clone Can Fool Family, Your Bank, But Not Your Video Meeting

By Wall Street Journal  
May 02, 2023 12:18 am



You can pay companies to create video and audio versions of yourself using generative artificial intelligence. But how well does it work? WSJ senior personal tech columnist Joanna Stern joins host Zoe Thomas to explain what it was like to work with her AI clone, and why it has her worried. Illustration: Amogh Alva Vaz/WSJ



Artificial Intelligence | May 2, 2023

By Sue Poremba | 4 min read

Share ↗

# What to consider

---

- Procurement Process
  - Due Diligence/Audits
  - Contractual Arrangements
  - Opt-out of re-use of data for training purposes
- Guardrails
  - Consumer Facing
    - Notices/Terms of Use/Disclaimers
  - Inputs/Outputs
  - Storage
    - What and How?
  - Staff Usage
    - Policies



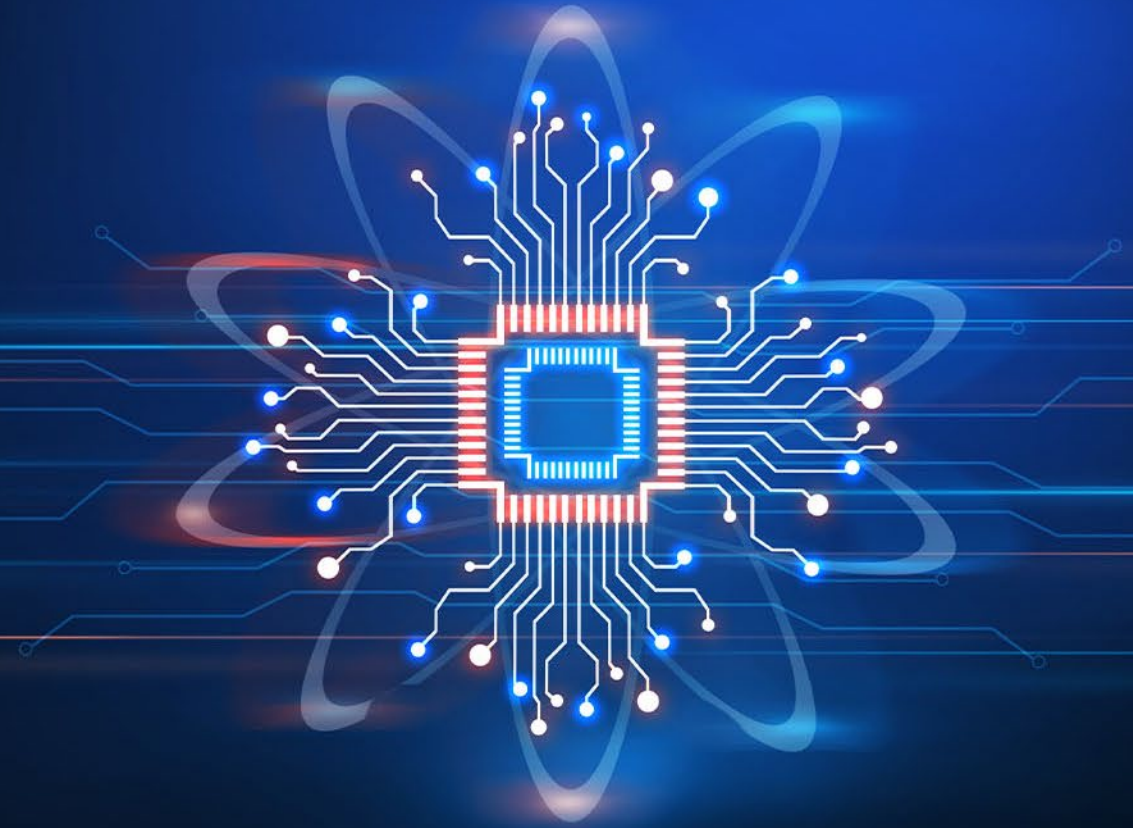
# Takeaways

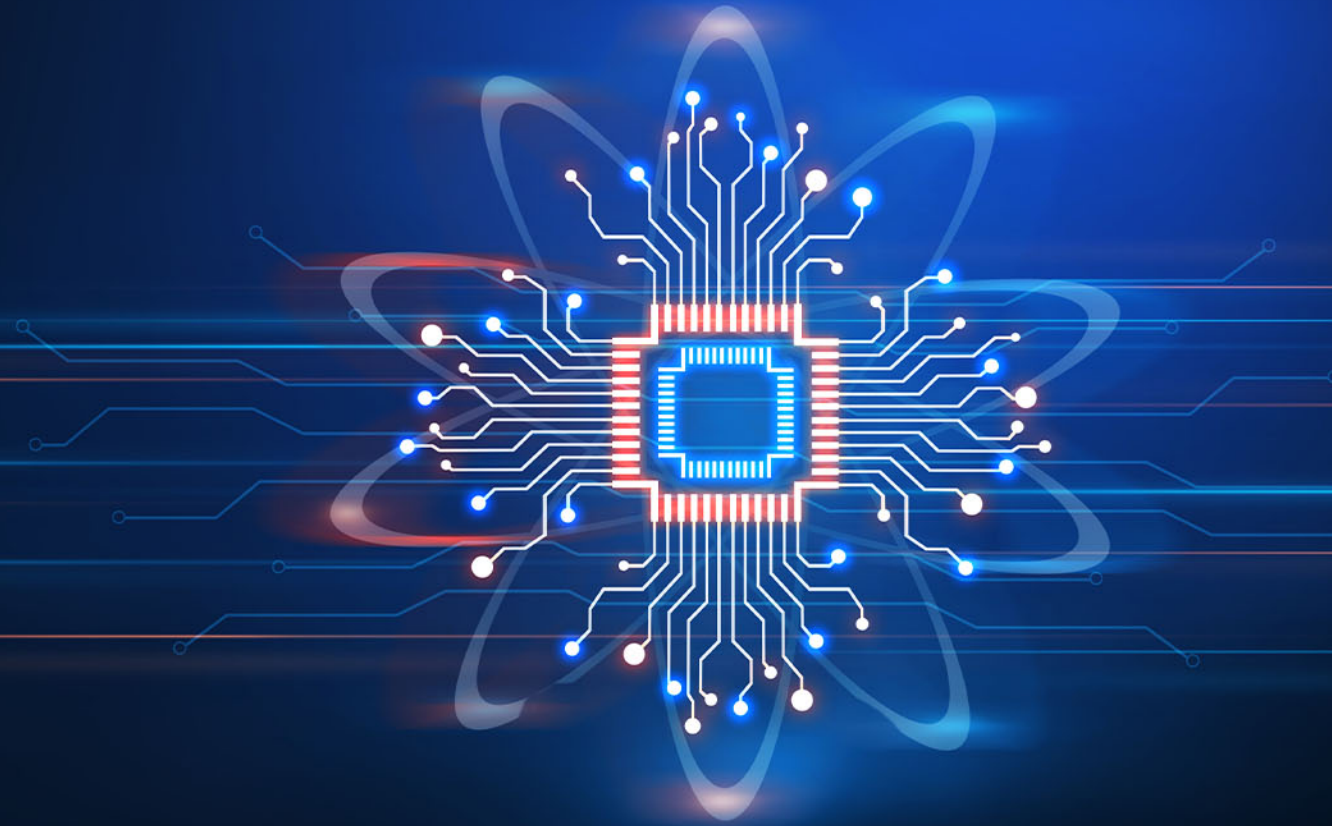
---

- Data Protection and Cybersecurity cannot be forgotten but it is not the only part of the picture
- Transparency is key
- Monitor for unintended consequences of AI use
- Global laws need to be considered
- AI is moving at a fast pace and governments/regulators are now trying to catch up so stay informed and constantly monitor legal development



Questions?





Proskauer»

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