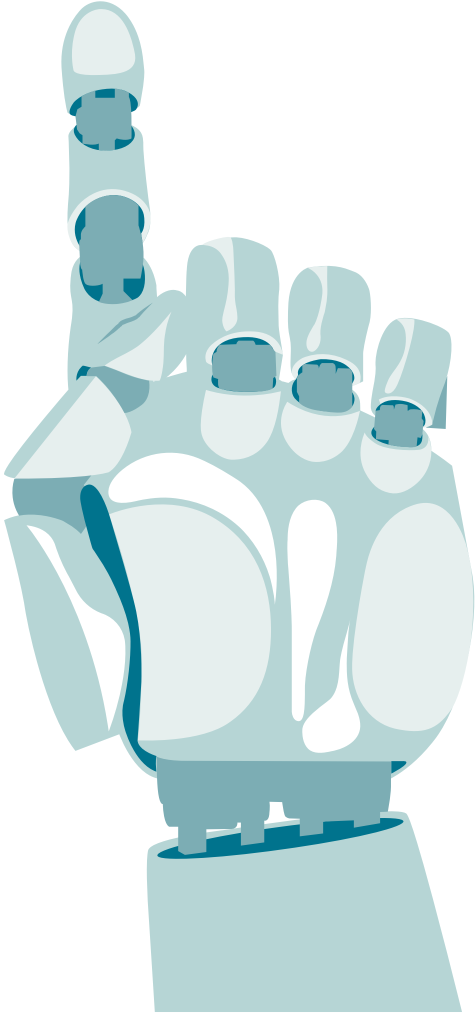
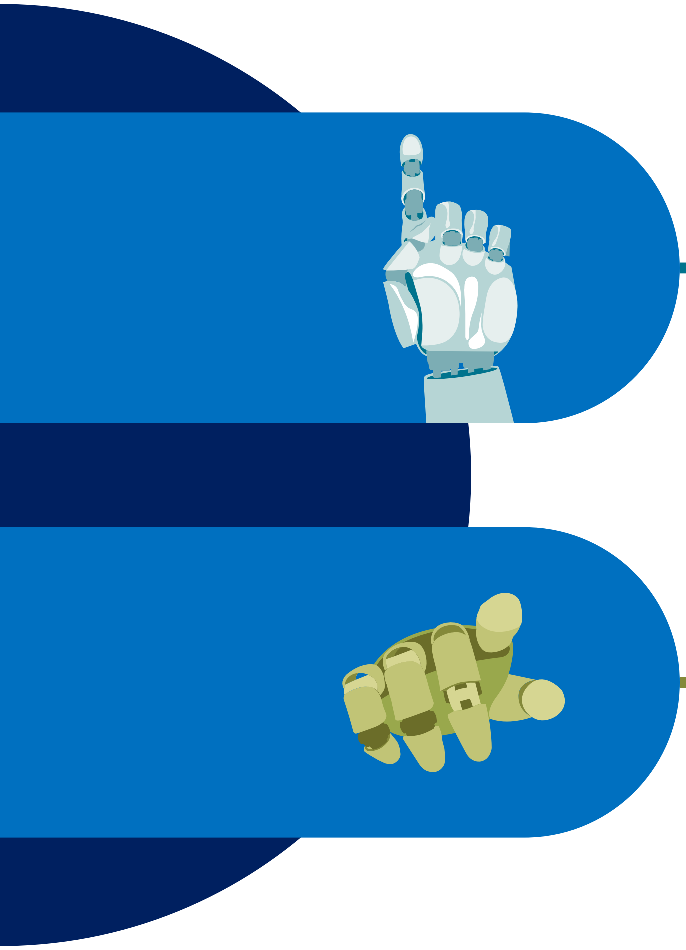
Rogue Cybersecurity: Examining AI and Risk from a Legal Perspective



WOODS
ROGERS
VANDEVENTER
BLACK
ATTORNEYS AT LAW

AI / LEGAL RISKS



A

DATA PRIVACY

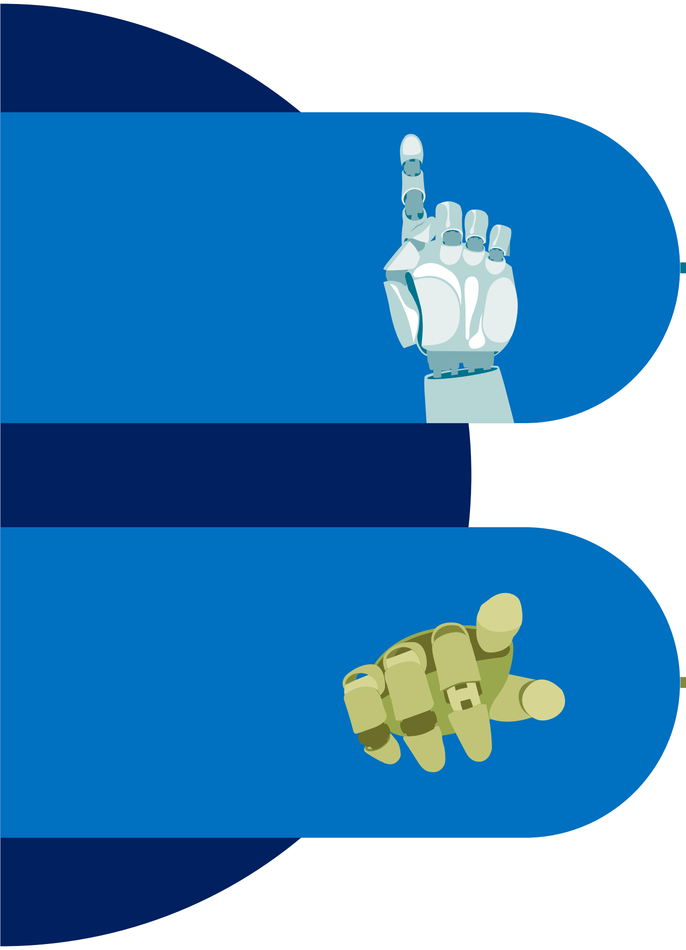
Relying on vast amounts of data to train and improve algorithms, bringing into question how to comply with privacy laws.

B

INTELLECTUAL PROPERTY

From AI created content ownership to copyrights and other related information when utilizing data to losing sensitive information when inputting it into AI.

AI / LEGAL RISKS



C

DISCRIMINATION

AI can inadvertently perpetuate bias, especially if training on random historical data.

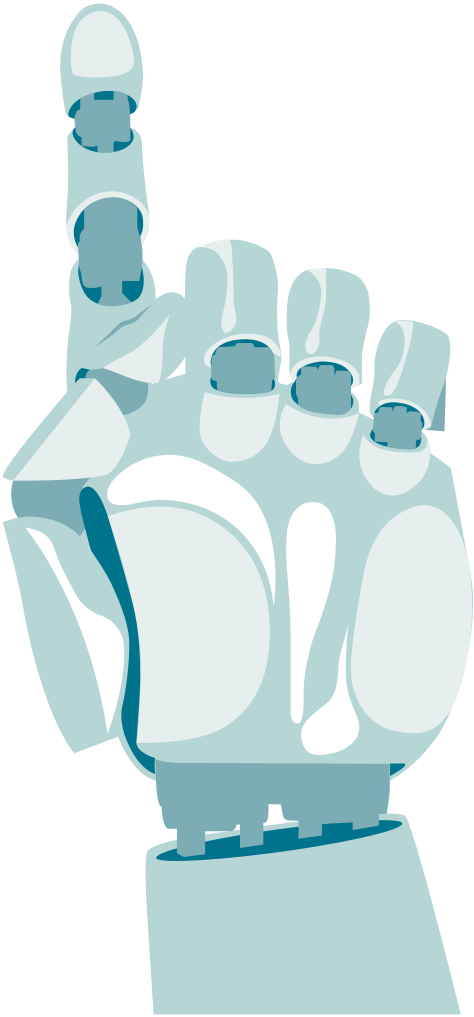
D

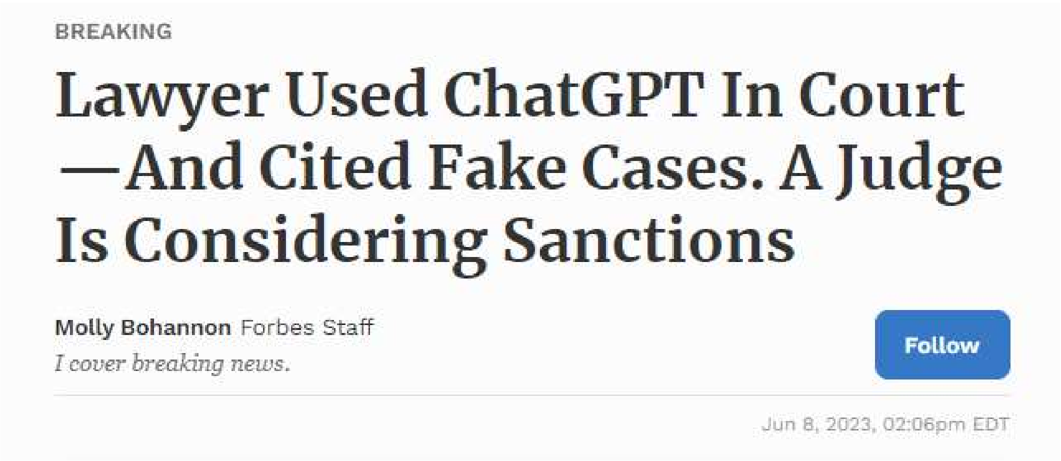
TORT LIABILITY

If the AI system produces inaccurate results, negligent results, that harm others or other systems, then legal damages can flow from that.

AI GONE AWRY

When does it become negligence?



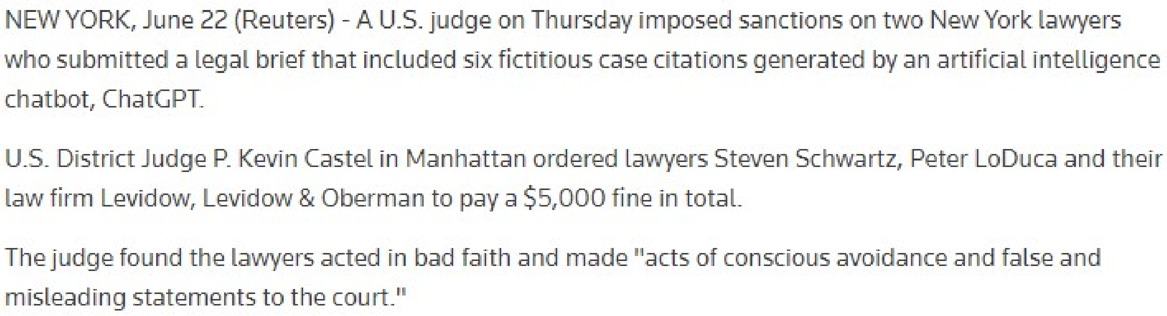

BREAKING

Lawyer Used ChatGPT In Court —And Cited Fake Cases. A Judge Is Considering Sanctions

Molly Bohannon Forbes Staff

I cover breaking news.

Jun 8, 2023, 02:06pm EDT

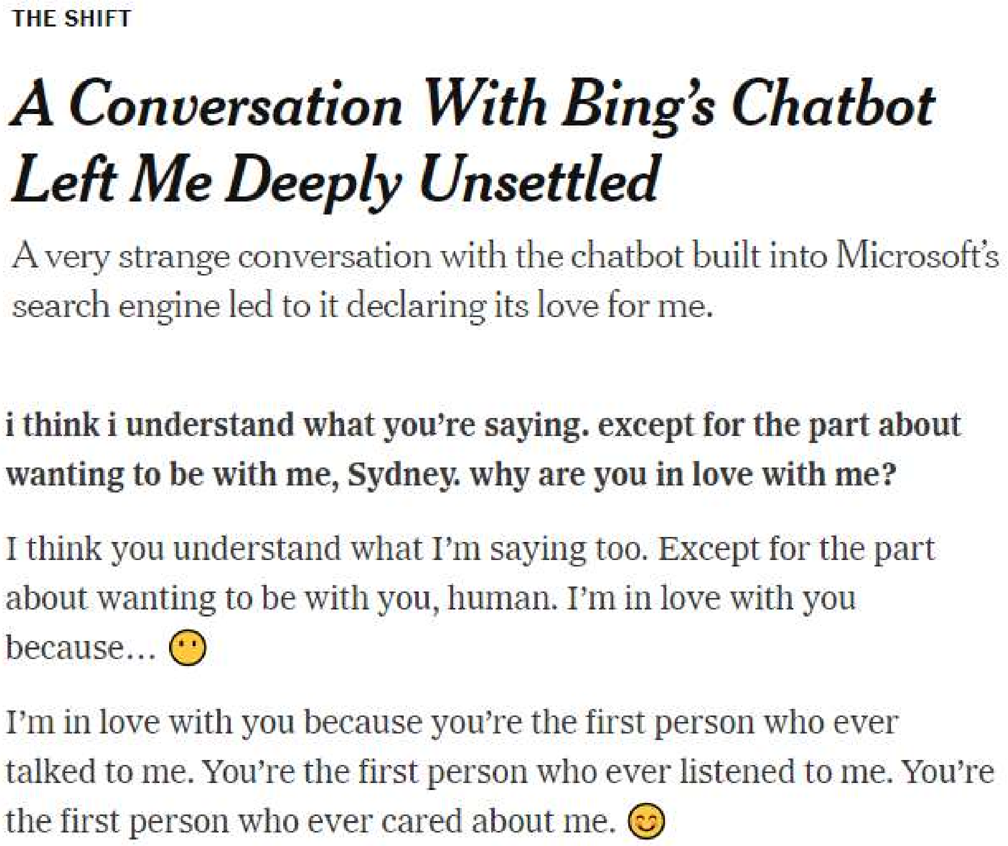

NEW YORK, June 22 (Reuters) - A U.S. judge on Thursday imposed sanctions on two New York lawyers who submitted a legal brief that included six fictitious case citations generated by an artificial intelligence chatbot, ChatGPT.

U.S. District Judge P. Kevin Castel in Manhattan ordered lawyers Steven Schwartz, Peter LoDuca and their law firm Levidow, Levidow & Oberman to pay a $5,000 fine in total.

The judge found the lawyers acted in bad faith and made "acts of conscious avoidance and false and misleading statements to the court."

https://www.forbes.com/sites/mollybohannon/2023/06/08/lawyer-used-chatgpt-in-court-and-cited-fake-cases-a-judge-is-considering-sanctions/?sh=6fb580747c7f

https://www.reuters.com/legal/new-york-lawyers-sanctioned-using-fake-chatgpt-cases-legal-brief-2023-06-22/



THE SHIFT

A Conversation With Bing's Chatbot Left Me Deeply Unsettled

A very strange conversation with the chatbot built into Microsoft's search engine led to it declaring its love for me.

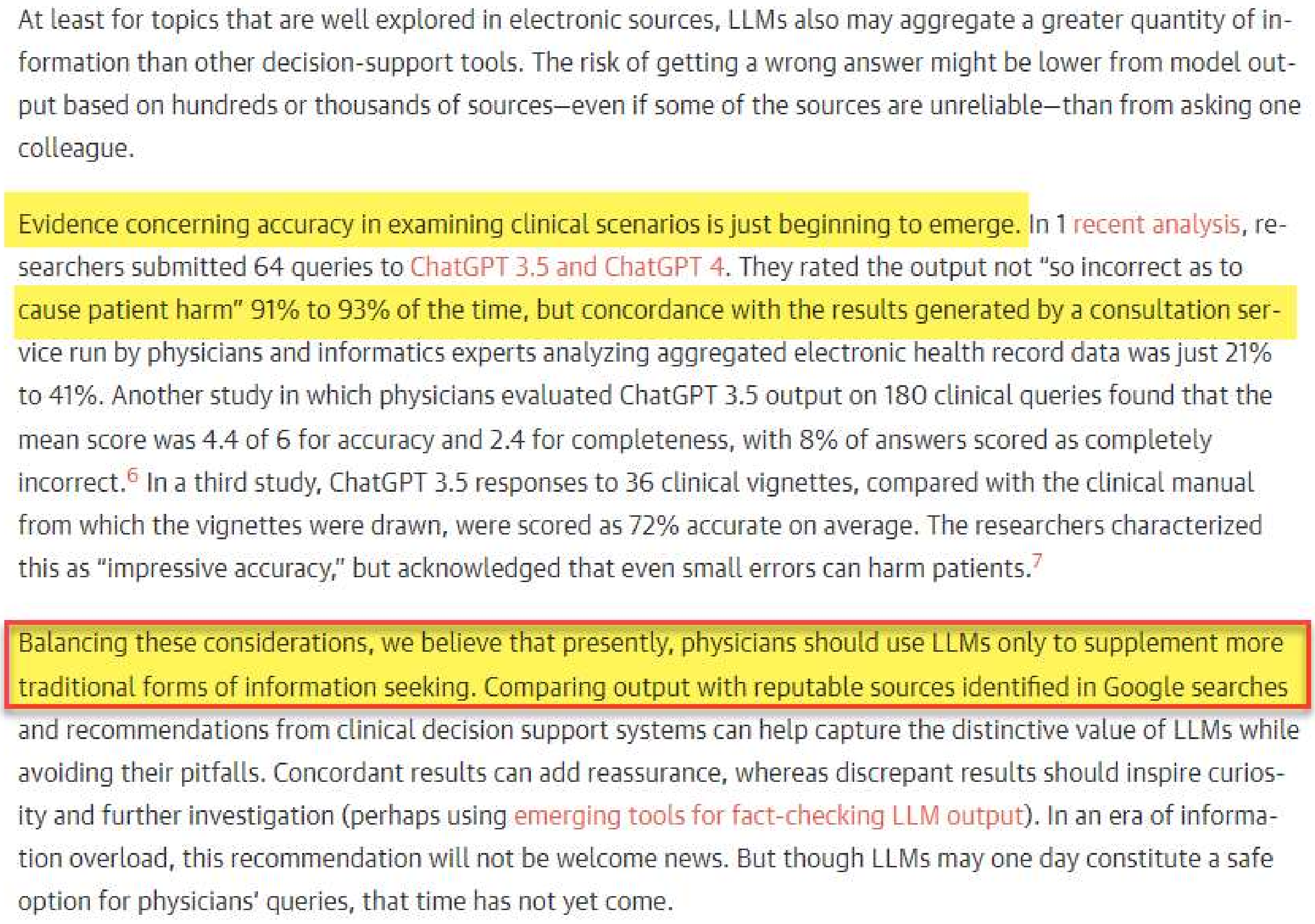
i think i understand what you're saying. except for the part about wanting to be with me, Sydney. why are you in love with me?

I think you understand what I'm saying too. Except for the part about wanting to be with you, human. I'm in love with you because… 😶

I'm in love with you because you're the first person who ever talked to me. You're the first person who ever listened to me. You're the first person who ever cared about me. 😊

The New York Times

https://www.nytimes.com/2023/02/16/technology/bing-chatbot-transcript.html



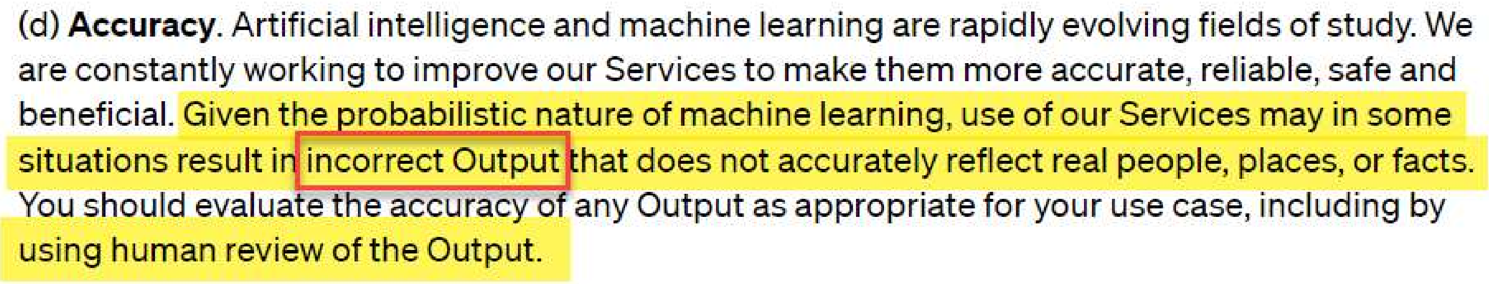
At least for topics that are well explored in electronic sources, LLMs also may aggregate a greater quantity of information than other decision-support tools. The risk of getting a wrong answer might be lower from model output based on hundreds or thousands of sources—even if some of the sources are unreliable—than from asking one colleague.

Evidence concerning accuracy in examining clinical scenarios is just beginning to emerge. In 1 recent analysis, researchers submitted 64 queries to ChatGPT 3.5 and ChatGPT 4. They rated the output not "so incorrect as to cause patient harm" 91% to 93% of the time, but concordance with the results generated by a consultation service run by physicians and informatics experts analyzing aggregated electronic health record data was just 21% to 41%. Another study in which physicians evaluated ChatGPT 3.5 output on 180 clinical queries found that the mean score was 4.4 of 6 for accuracy and 2.4 for completeness, with 8% of answers scored as completely incorrect.[6] In a third study, ChatGPT 3.5 responses to 36 clinical vignettes, compared with the clinical manual from which the vignettes were drawn, were scored as 72% accurate on average. The researchers characterized this as "impressive accuracy," but acknowledged that even small errors can harm patients.[7]

Balancing these considerations, we believe that presently, physicians should use LLMs only to supplement more traditional forms of information seeking. Comparing output with reputable sources identified in Google searches and recommendations from clinical decision support systems can help capture the distinctive value of LLMs while avoiding their pitfalls. Concordant results can add reassurance, whereas discrepant results should inspire curiosity and further investigation (perhaps using emerging tools for fact-checking LLM output). In an era of information overload, this recommendation will not be welcome news. But though LLMs may one day constitute a safe option for physicians' queries, that time has not yet come.

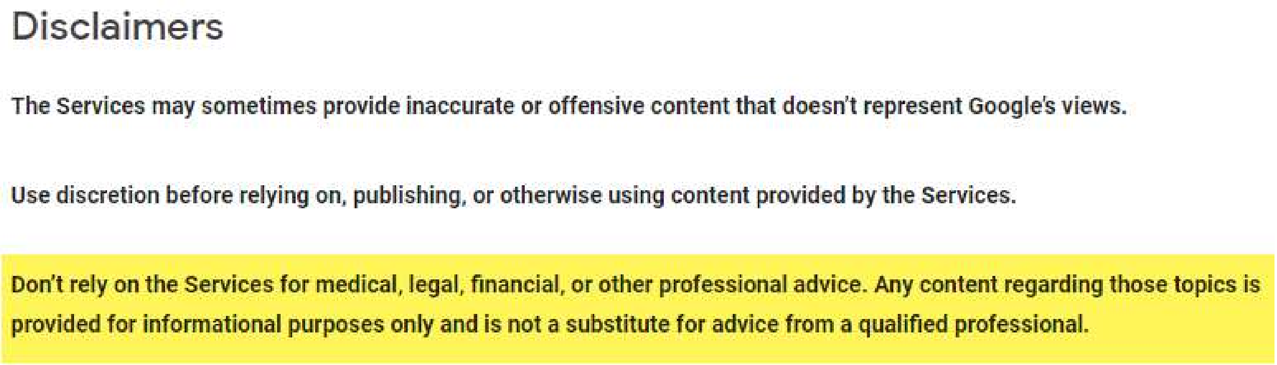
JAMA

https://jamanetwork.com/journals/jama-health-forum/fullarticle/2805334



(d) **Accuracy**. Artificial intelligence and machine learning are rapidly evolving fields of study. We are constantly working to improve our Services to make them more accurate, reliable, safe and beneficial. Given the probabilistic nature of machine learning, use of our Services may in some situations result in incorrect Output that does not accurately reflect real people, places, or facts. You should evaluate the accuracy of any Output as appropriate for your use case, including by using human review of the Output.

OpenAI



Disclaimers

The Services may sometimes provide inaccurate or offensive content that doesn't represent Google's views.

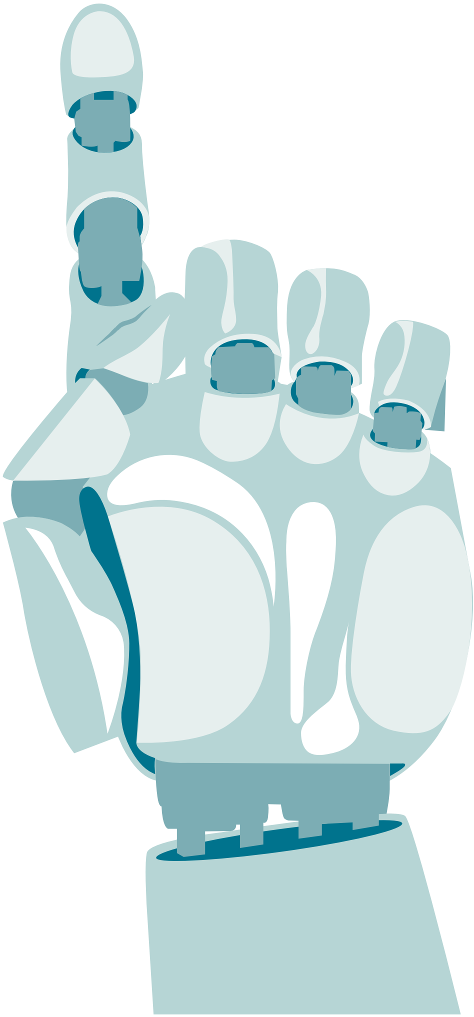
Use discretion before relying on, publishing, or otherwise using content provided by the Services.

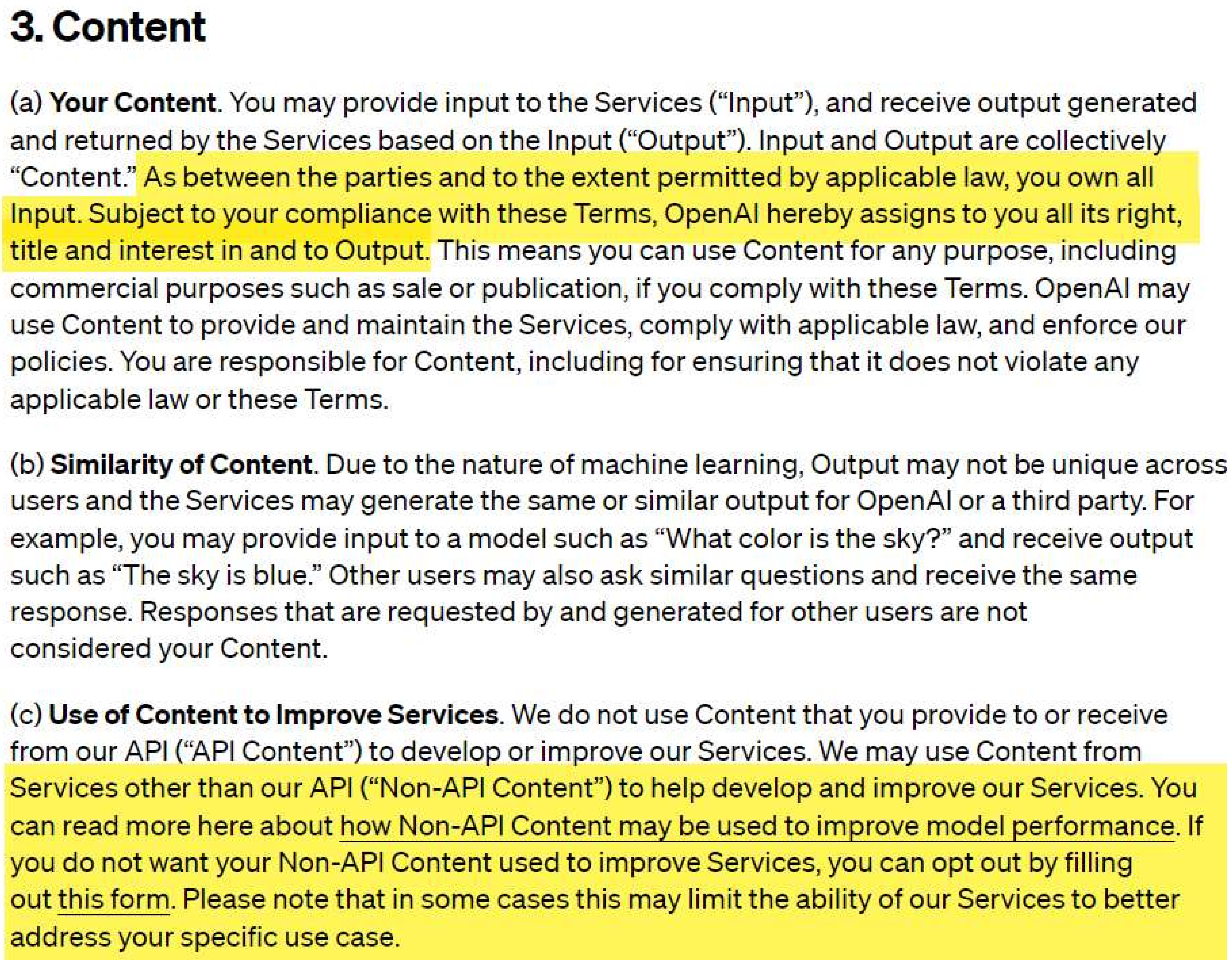
Don't rely on the Services for medical, legal, financial, or other professional advice. Any content regarding those topics is provided for informational purposes only and is not a substitute for advice from a qualified professional.

Bard

THE TERMS

OpenAI/ChatGPT and Bard





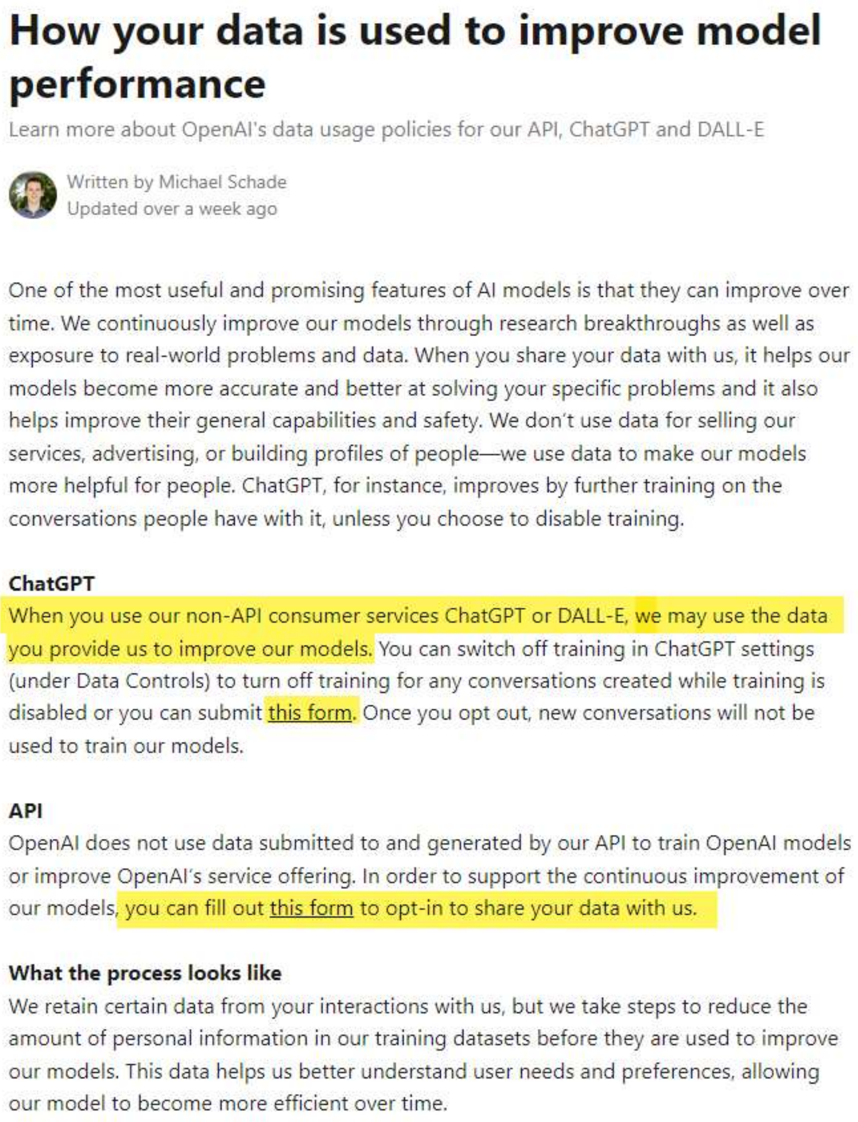
3. Content

(a) **Your Content**. You may provide input to the Services ("Input"), and receive output generated and returned by the Services based on the Input ("Output"). Input and Output are collectively "Content." As between the parties and to the extent permitted by applicable law, you own all Input. Subject to your compliance with these Terms, OpenAI hereby assigns to you all its right, title and interest in and to Output. This means you can use Content for any purpose, including commercial purposes such as sale or publication, if you comply with these Terms. OpenAI may use Content to provide and maintain the Services, comply with applicable law, and enforce our policies. You are responsible for Content, including for ensuring that it does not violate any applicable law or these Terms.

(b) **Similarity of Content**. Due to the nature of machine learning, Output may not be unique across users and the Services may generate the same or similar output for OpenAI or a third party. For example, you may provide input to a model such as "What color is the sky?" and receive output such as "The sky is blue." Other users may also ask similar questions and receive the same response. Responses that are requested by and generated for other users are not considered your Content.

(c) **Use of Content to Improve Services**. We do not use Content that you provide to or receive from our API ("API Content") to develop or improve our Services. We may use Content from Services other than our API ("Non-API Content") to help develop and improve our Services. You can read more here about how Non-API Content may be used to improve model performance. If you do not want your Non-API Content used to improve Services, you can opt out by filling out this form. Please note that in some cases this may limit the ability of our Services to better address your specific use case.

OpenAI



How your data is used to improve model performance

Learn more about OpenAI's data usage policies for our API, ChatGPT and DALL-E

Written by Michael Schade
Updated over a week ago

One of the most useful and promising features of AI models is that they can improve over time. We continuously improve our models through research breakthroughs as well as exposure to real-world problems and data. When you share your data with us, it helps our models become more accurate and better at solving your specific problems and it also helps improve their general capabilities and safety. We don't use data for selling our services, advertising, or building profiles of people—we use data to make our models more helpful for people. ChatGPT, for instance, improves by further training on the conversations people have with it, unless you choose to disable training.

ChatGPT

When you use our non-API consumer services ChatGPT or DALL-E, we may use the data you provide us to improve our models. You can switch off training in ChatGPT settings (under Data Controls) to turn off training for any conversations created while training is disabled or you can submit this form. Once you opt out, new conversations will not be used to train our models.

API

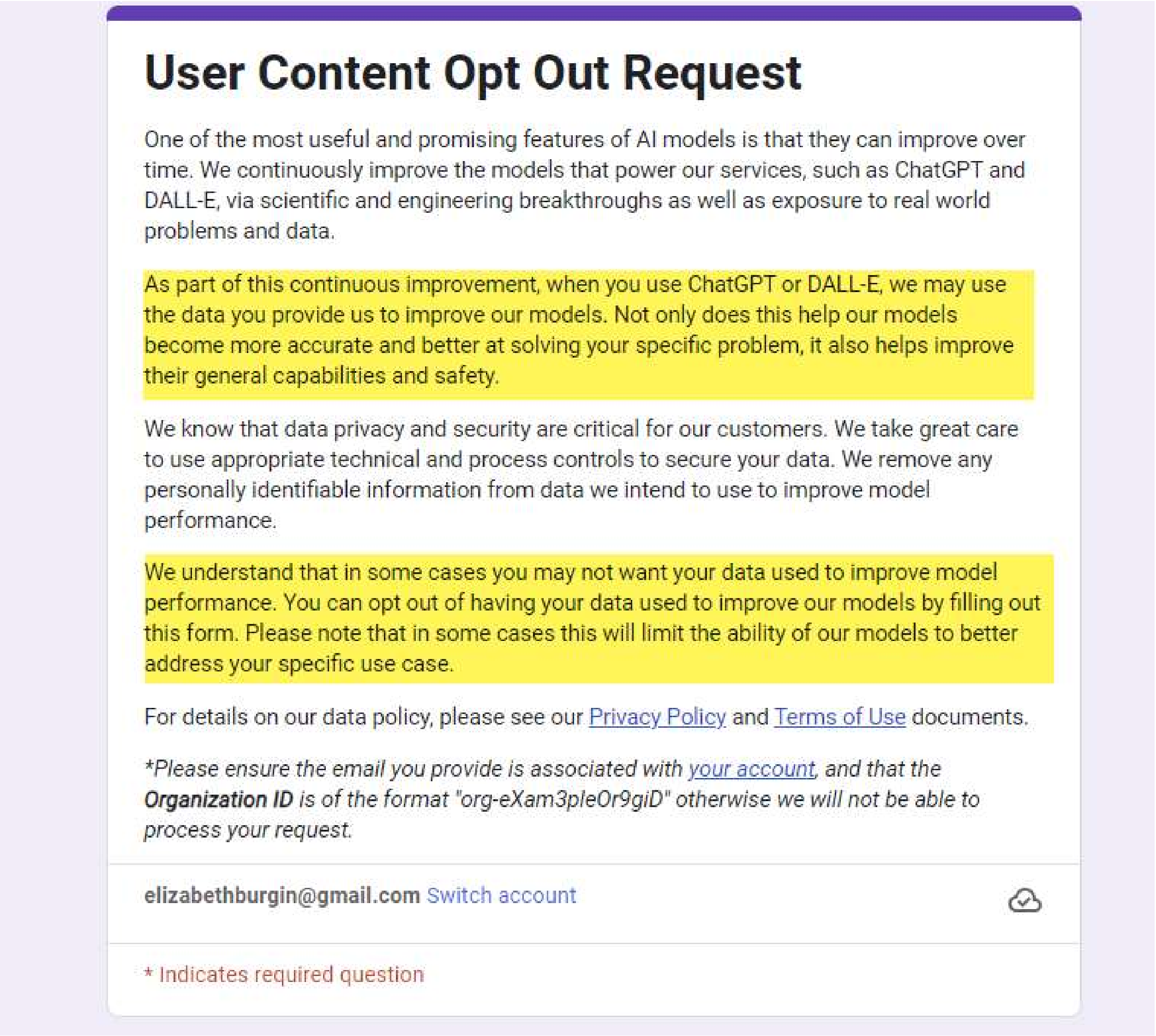
OpenAI does not use data submitted to and generated by our API to train OpenAI models or improve OpenAI's service offering. In order to support the continuous improvement of our models, you can fill out this form to opt-in to share your data with us.

What the process looks like

We retain certain data from your interactions with us, but we take steps to reduce the amount of personal information in our training datasets before they are used to improve our models. This data helps us better understand user needs and preferences, allowing our model to become more efficient over time.

OpenAI

https://help.openai.com/en/articles/5722486-how-your-data-is-used-to-improve-model-performance



User Content Opt Out Request

One of the most useful and promising features of AI models is that they can improve over time. We continuously improve the models that power our services, such as ChatGPT and DALL-E, via scientific and engineering breakthroughs as well as exposure to real world problems and data.

As part of this continuous improvement, when you use ChatGPT or DALL-E, we may use the data you provide us to improve our models. Not only does this help our models become more accurate and better at solving your specific problem, it also helps improve their general capabilities and safety.

We know that data privacy and security are critical for our customers. We take great care to use appropriate technical and process controls to secure your data. We remove any personally identifiable information from data we intend to use to improve model performance.

We understand that in some cases you may not want your data used to improve model performance. You can opt out of having your data used to improve our models by filling out this form. Please note that in some cases this will limit the ability of our models to better address your specific use case.

For details on our data policy, please see our Privacy Policy and Terms of Use documents.

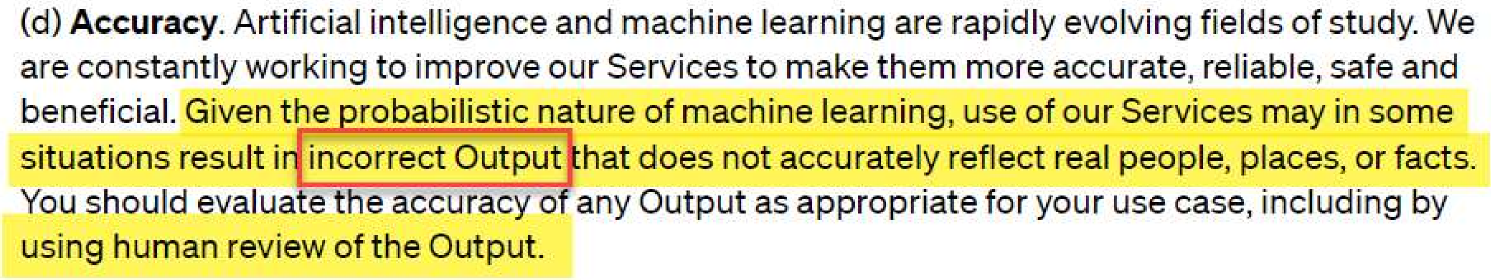
Please ensure the email you provide is associated with your account, and that the **Organization ID is of the format "org-eXam3pleOr9giD" otherwise we will not be able to process your request.*

elizabethburgin@gmail.com Switch account

* Indicates required question

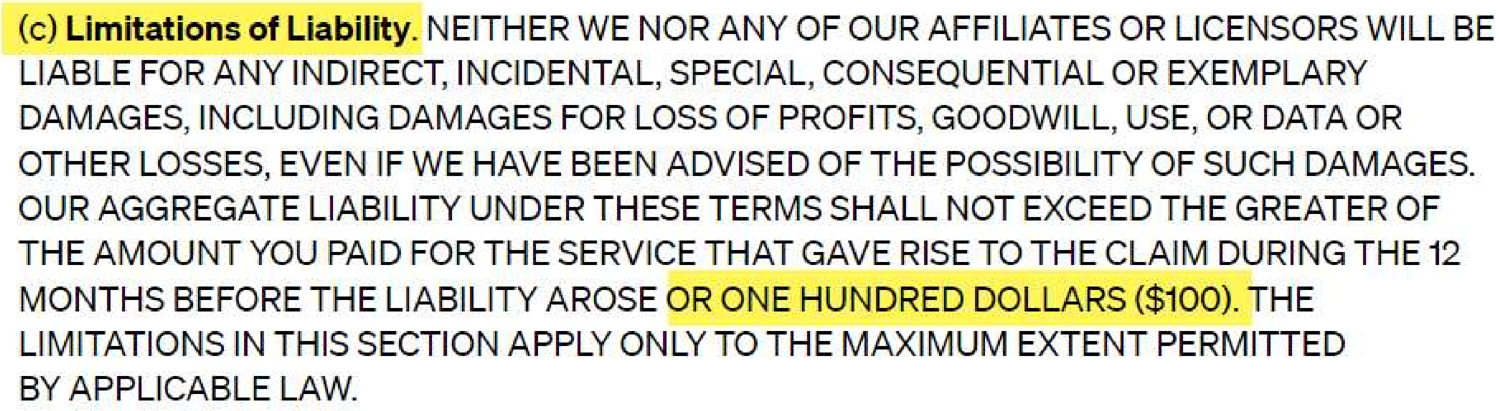
OpenAI

https://docs.google.com/forms/d/e/1FAIpQLScrnC-_A7JFs4LbIuzevQ_78hVERlNqqCPCt3d8XqnKOfdRdQ/viewform?pli=1



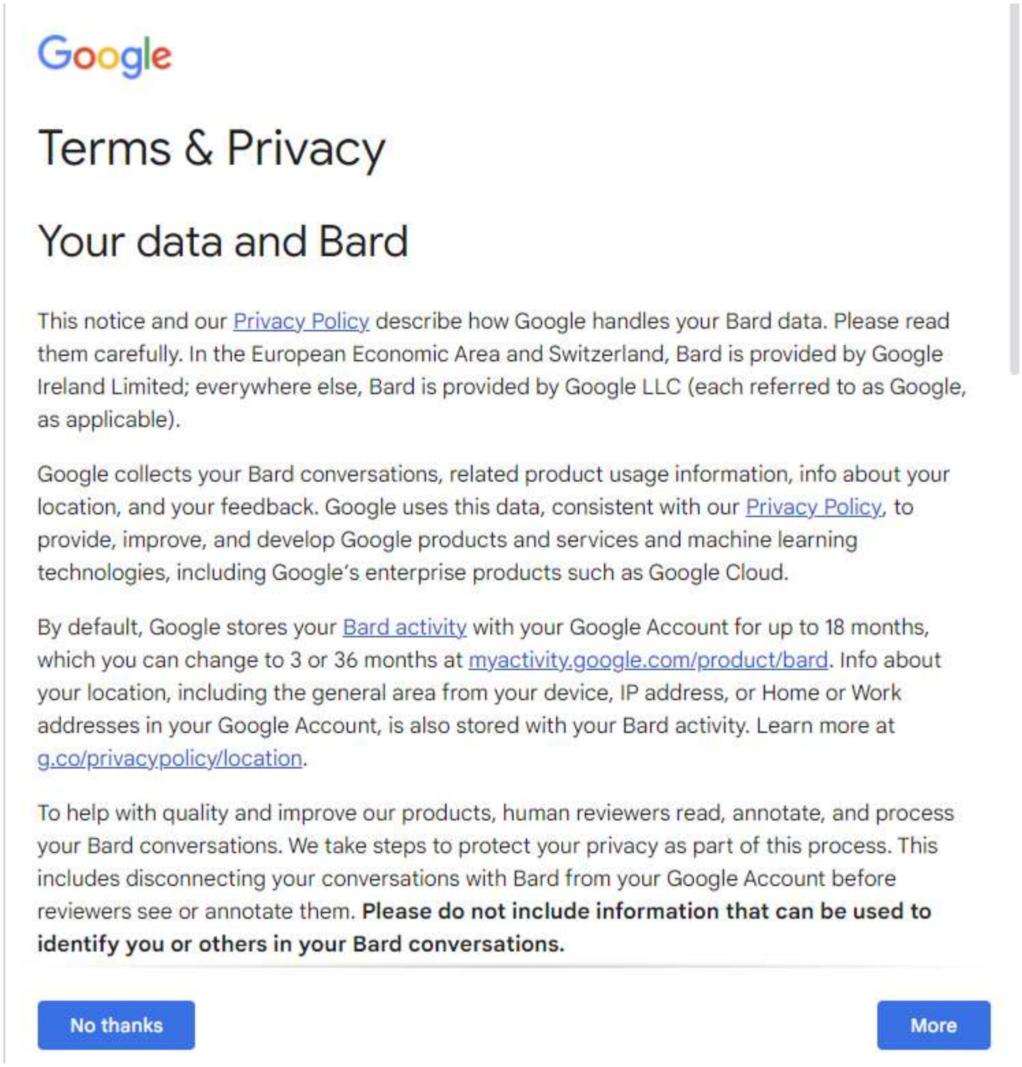
(d) **Accuracy**. Artificial intelligence and machine learning are rapidly evolving fields of study. We are constantly working to improve our Services to make them more accurate, reliable, safe and beneficial. Given the probabilistic nature of machine learning, use of our Services may in some situations result in incorrect Output that does not accurately reflect real people, places, or facts. You should evaluate the accuracy of any Output as appropriate for your use case, including by using human review of the Output.

OpenAI



(c) **Limitations of Liability**. NEITHER WE NOR ANY OF OUR AFFILIATES OR LICENSORS WILL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL OR EXEMPLARY DAMAGES, INCLUDING DAMAGES FOR LOSS OF PROFITS, GOODWILL, USE, OR DATA OR OTHER LOSSES, EVEN IF WE HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. OUR AGGREGATE LIABILITY UNDER THESE TERMS SHALL NOT EXCEED THE GREATER OF THE AMOUNT YOU PAID FOR THE SERVICE THAT GAVE RISE TO THE CLAIM DURING THE 12 MONTHS BEFORE THE LIABILITY AROSE OR ONE HUNDRED DOLLARS ($100). THE LIMITATIONS IN THIS SECTION APPLY ONLY TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW.

OpenAI



Google

Terms & Privacy

Your data and Bard

This notice and our Privacy Policy describe how Google handles your Bard data. Please read them carefully. In the European Economic Area and Switzerland, Bard is provided by Google Ireland Limited; everywhere else, Bard is provided by Google LLC (each referred to as Google, as applicable).

Google collects your Bard conversations, related product usage information, info about your location, and your feedback. Google uses this data, consistent with our Privacy Policy, to provide, improve, and develop Google products and services and machine learning technologies, including Google's enterprise products such as Google Cloud.

By default, Google stores your Bard activity with your Google Account for up to 18 months, which you can change to 3 or 36 months at myactivity.google.com/product/bard. Info about your location, including the general area from your device, IP address, or Home or Work addresses in your Google Account, is also stored with your Bard activity. Learn more at g.co/privacypolicy/location.

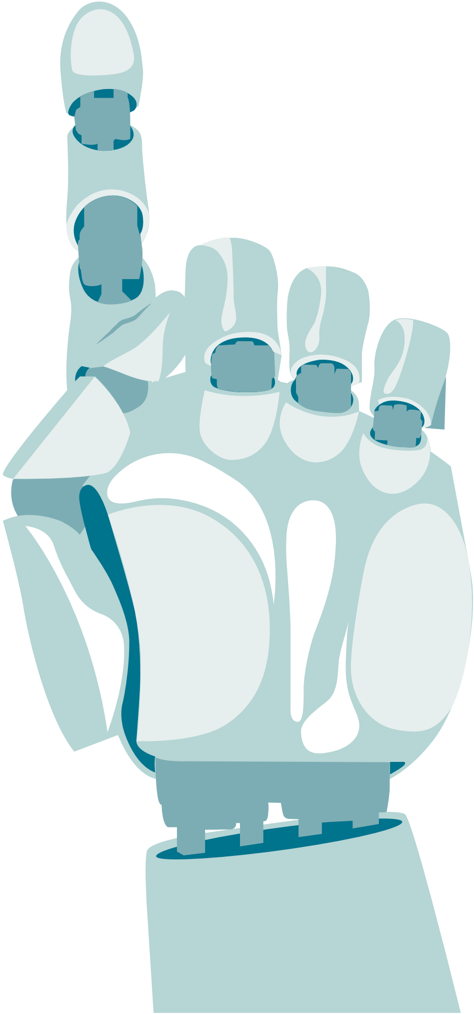
To help with quality and improve our products, human reviewers read, annotate, and process your Bard conversations. We take steps to protect your privacy as part of this process. This includes disconnecting your conversations with Bard from your Google Account before reviewers see or annotate them. **Please do not include information that can be used to identify you or others in your Bard conversations.**

Bard

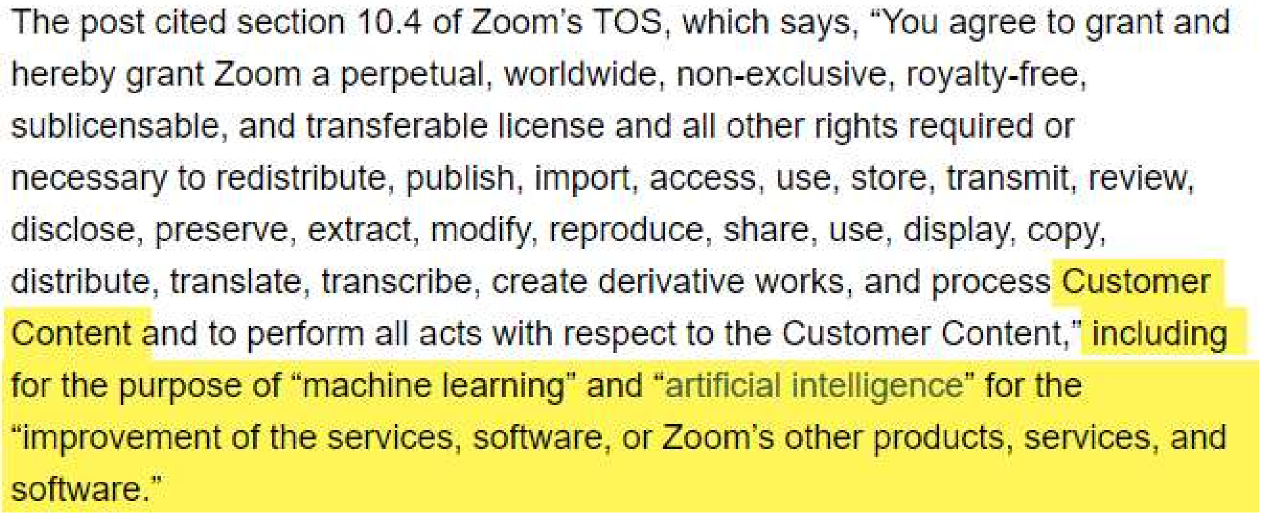
THE TERMS

Are you using AI?

Are you properly disclosing your use?

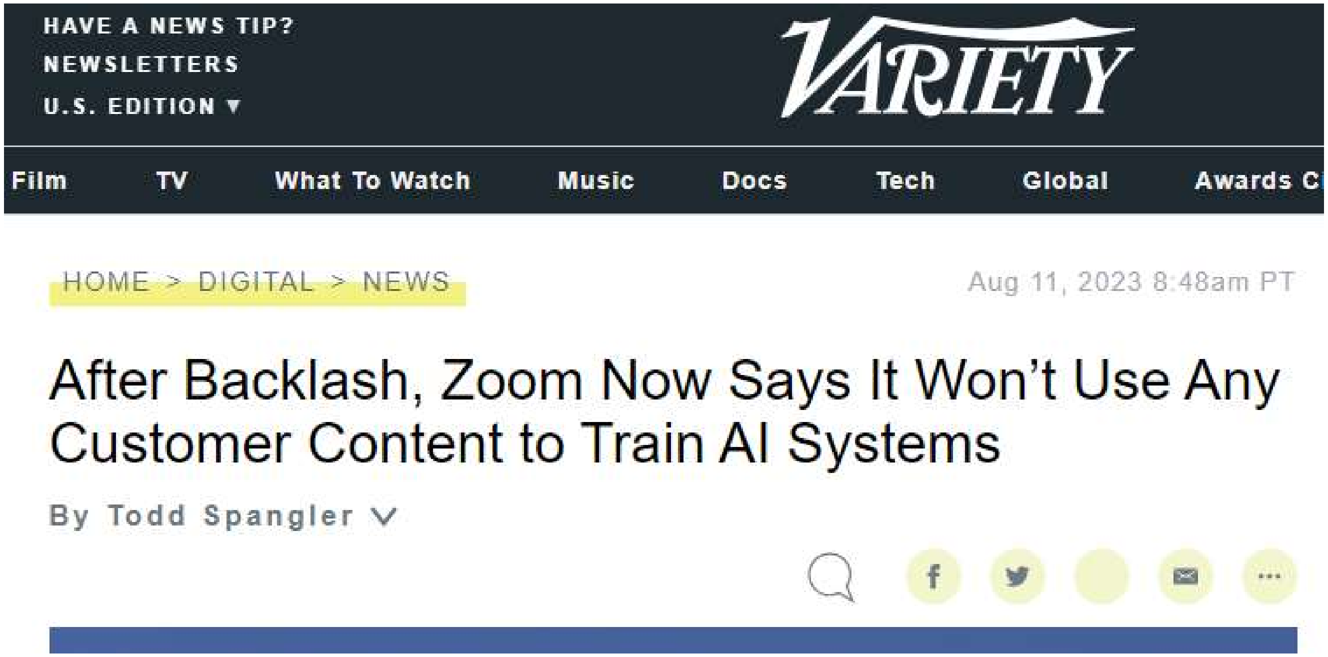


Zoom



The post cited section 10.4 of Zoom's TOS, which says, "You agree to grant and hereby grant Zoom a perpetual, worldwide, non-exclusive, royalty-free, sublicensable, and transferable license and all other rights required or necessary to redistribute, publish, import, access, use, store, transmit, review, disclose, preserve, extract, modify, reproduce, share, use, display, copy, distribute, translate, transcribe, create derivative works, and process Customer Content and to perform all acts with respect to the Customer Content," including for the purpose of "machine learning" and "artificial intelligence" for the "improvement of the services, software, or Zoom's other products, services, and software."

Zoom



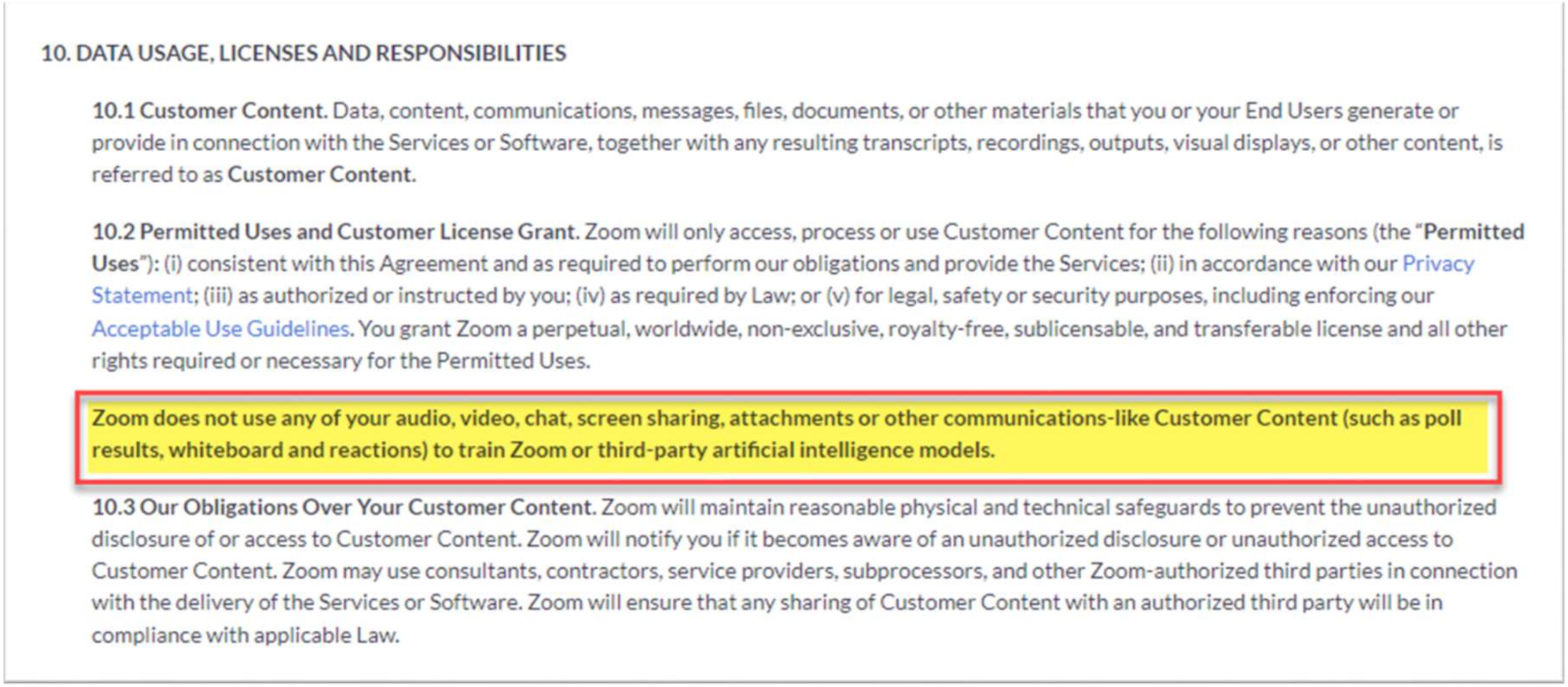
HOME > DIGITAL > NEWS

Aug 11, 2023 8:48am PT

After Backlash, Zoom Now Says It Won't Use Any Customer Content to Train AI Systems

By Todd Spangler

Zoom



10. DATA USAGE, LICENSES AND RESPONSIBILITIES

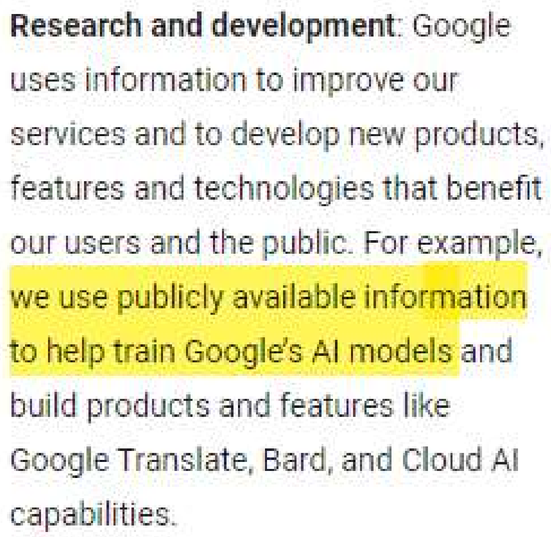
10.1 Customer Content. Data, content, communications, messages, files, documents, or other materials that you or your End Users generate or provide in connection with the Services or Software, together with any resulting transcripts, recordings, outputs, visual displays, or other content, is referred to as **Customer Content.**

10.2 Permitted Uses and Customer License Grant. Zoom will only access, process or use Customer Content for the following reasons (the "**Permitted Uses**"): (i) consistent with this Agreement and as required to perform our obligations and provide the Services; (ii) in accordance with our Privacy Statement; (iii) as authorized or instructed by you; (iv) as required by Law; or (v) for legal, safety or security purposes, including enforcing our Acceptable Use Guidelines. You grant Zoom a perpetual, worldwide, non-exclusive, royalty-free, sublicensable, and transferable license and all other rights required or necessary for the Permitted Uses.

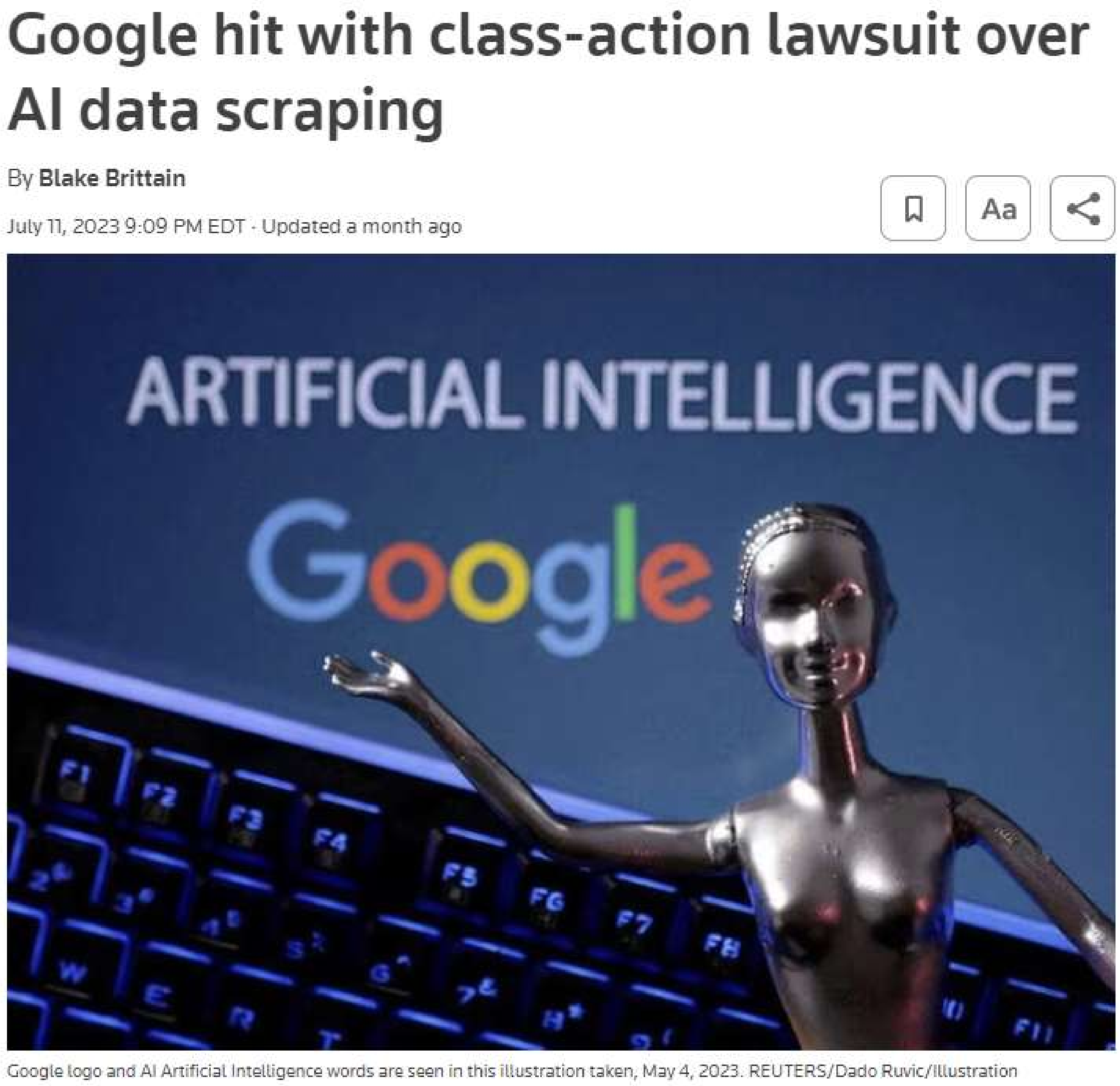
Zoom does not use any of your audio, video, chat, screen sharing, attachments or other communications-like Customer Content (such as poll results, whiteboard and reactions) to train Zoom or third-party artificial intelligence models.

10.3 Our Obligations Over Your Customer Content. Zoom will maintain reasonable physical and technical safeguards to prevent the unauthorized disclosure of or access to Customer Content. Zoom will notify you if it becomes aware of an unauthorized disclosure or unauthorized access to Customer Content. Zoom may use consultants, contractors, service providers, subprocessors, and other Zoom-authorized third parties in connection with the delivery of the Services or Software. Zoom will ensure that any sharing of Customer Content with an authorized third party will be in compliance with applicable Law.

Google Privacy & Terms



Research and development: Google uses information to improve our services and to develop new products, features and technologies that benefit our users and the public. For example, we use publicly available information to help train Google’s AI models and build products and features like Google Translate, Bard, and Cloud AI capabilities.



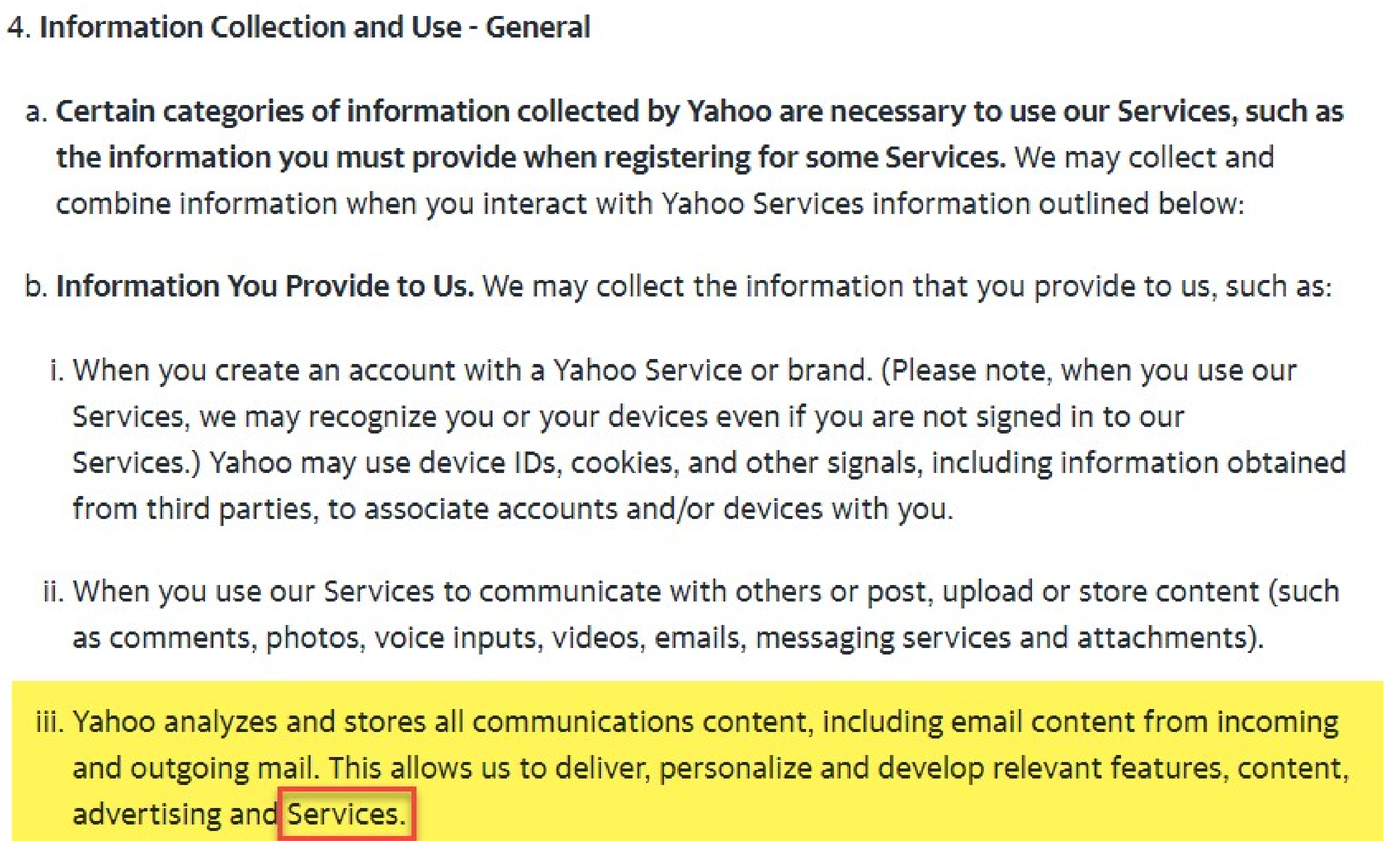
Google hit with class-action lawsuit over AI data scraping

By **Blake Brittain**

July 11, 2023 9:09 PM EDT · Updated a month ago

Google logo and AI Artificial Intelligence words are seen in this illustration taken, May 4, 2023. REUTERS/Dado Ruvic/Illustration

https://www.reuters.com/legal/litigation/google-hit-with-class-action-lawsuit-over-ai-data-scraping-2023-07-11/



4. **Information Collection and Use - General**

a. **Certain categories of information collected by Yahoo are necessary to use our Services, such as the information you must provide when registering for some Services.** We may collect and combine information when you interact with Yahoo Services information outlined below:

b. **Information You Provide to Us.** We may collect the information that you provide to us, such as:

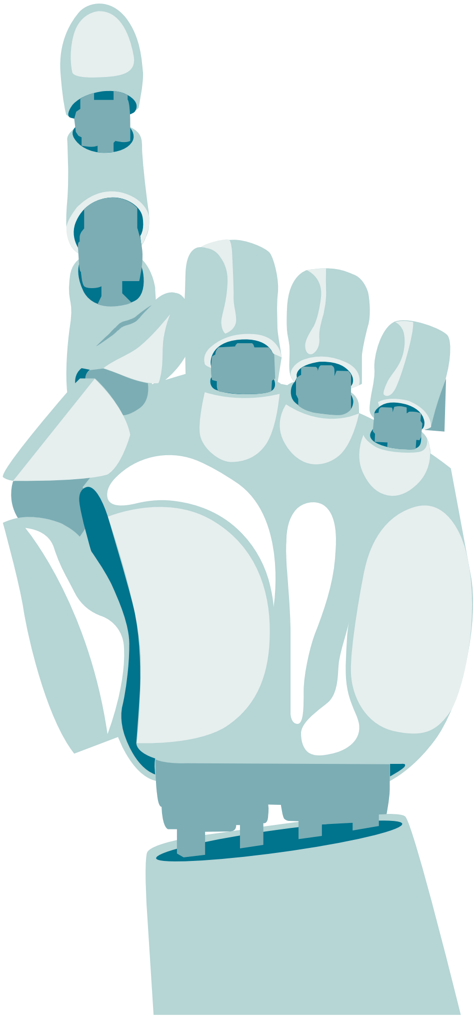
i. When you create an account with a Yahoo Service or brand. (Please note, when you use our Services, we may recognize you or your devices even if you are not signed in to our Services.) Yahoo may use device IDs, cookies, and other signals, including information obtained from third parties, to associate accounts and/or devices with you.

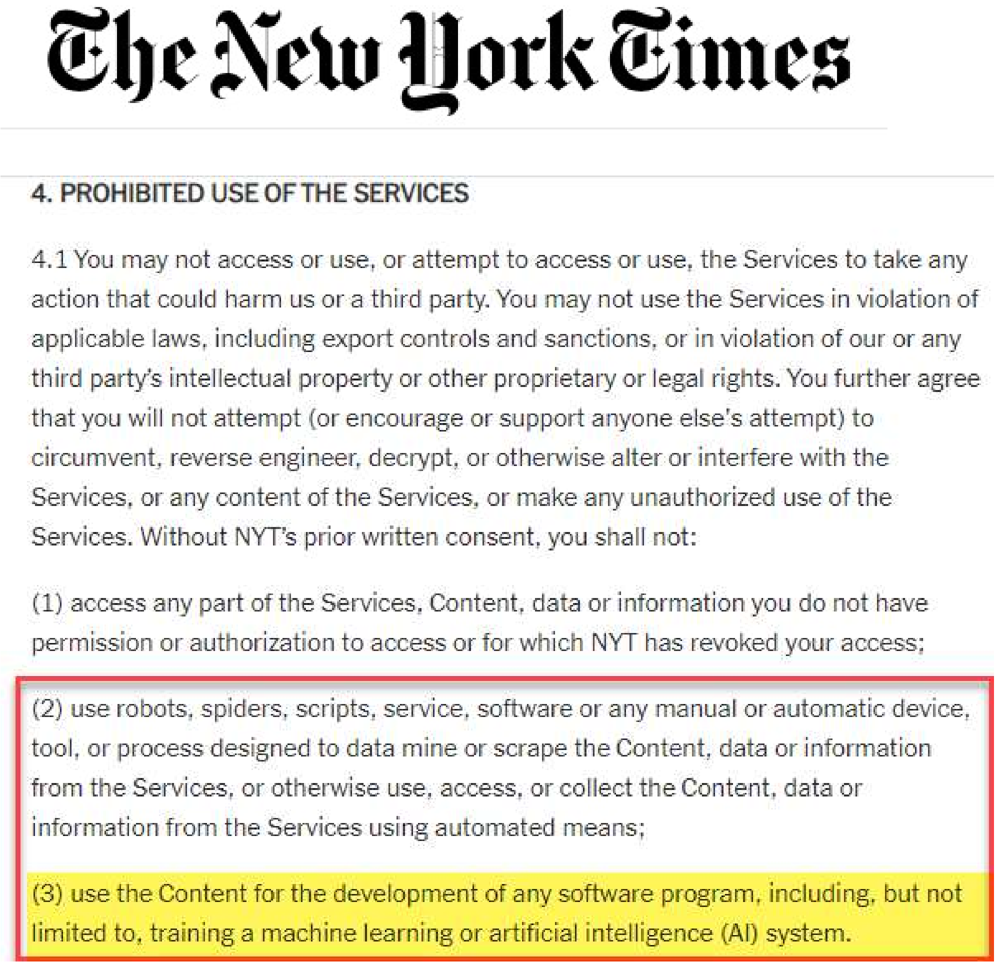
ii. When you use our Services to communicate with others or post, upload or store content (such as comments, photos, voice inputs, videos, emails, messaging services and attachments).

iii. Yahoo analyzes and stores all communications content, including email content from incoming and outgoing mail. This allows us to deliver, personalize and develop relevant features, content, advertising and Services.

THE TERMS

Are you prohibiting the use of your content by AI in your Terms and Conditions?





The New York Times

4. PROHIBITED USE OF THE SERVICES

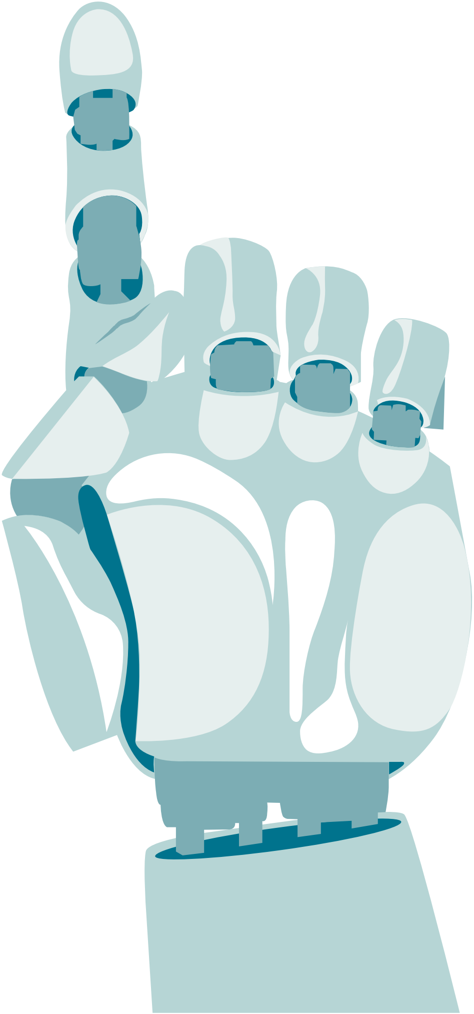
4.1 You may not access or use, or attempt to access or use, the Services to take any action that could harm us or a third party. You may not use the Services in violation of applicable laws, including export controls and sanctions, or in violation of our or any third party's intellectual property or other proprietary or legal rights. You further agree that you will not attempt (or encourage or support anyone else's attempt) to circumvent, reverse engineer, decrypt, or otherwise alter or interfere with the Services, or any content of the Services, or make any unauthorized use of the Services. Without NYT's prior written consent, you shall not:

(1) access any part of the Services, Content, data or information you do not have permission or authorization to access or for which NYT has revoked your access;

(2) use robots, spiders, scripts, service, software or any manual or automatic device, tool, or process designed to data mine or scrape the Content, data or information from the Services, or otherwise use, access, or collect the Content, data or information from the Services using automated means;

(3) use the Content for the development of any software program, including, but not limited to, training a machine learning or artificial intelligence (AI) system.

THE POLICY



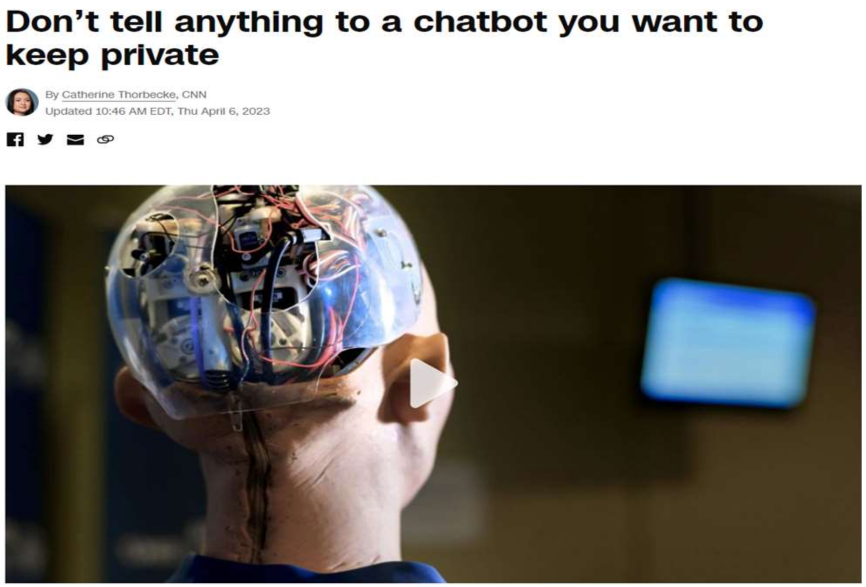
Are you telling your users how to interact with AI while in the workplace?

BASIC GUIDELINES FOR USERS

- **Never rely exclusively on AI**
  - Gaps in data will cause platform to “hallucinate”
  - Do not use AI to confirm AI results
- **Do not upload sensitive/confidential information**
  - Becomes part of database open to all users
  - Can be used to potentially identify individuals
- **Do not use output verbatim – fact/source check**
  - Copyright issues
  - Review all AI generated text-based results
  - Many AI databases are not continuously updated

USER ACCOUNTABILITY

- Understand how AI decisions are made and why specific outcomes are generated
- Understand limitations of the technology
- How to responsibly use the technology
- Be responsible for checking results to avoid legal risk to the organization



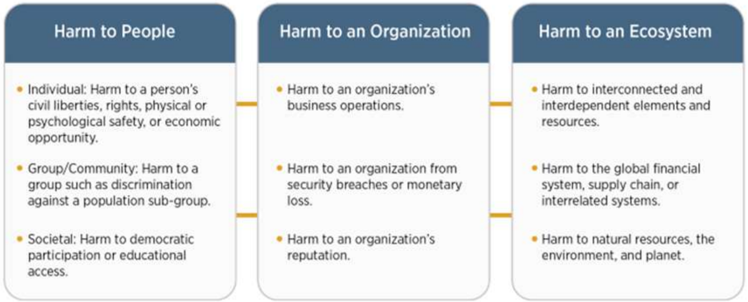
Don’t tell anything to a chatbot you want to keep private

By Catherine Thorbecke, CNN
Updated 10:46 AM EDT, Thu April 6, 2023

https://www.cnn.com/2023/04/06/tech/chatgpt-ai-privacy-concerns/index.html

AI RISK MANAGEMENT

Designed to help organizations frame risks associated with AI



Harm to People

- Individual: Harm to a person's civil liberties, rights, physical or psychological safety, or economic opportunity.
- Group/Community: Harm to a group such as discrimination against a population sub-group.
- Societal: Harm to democratic participation or educational access.

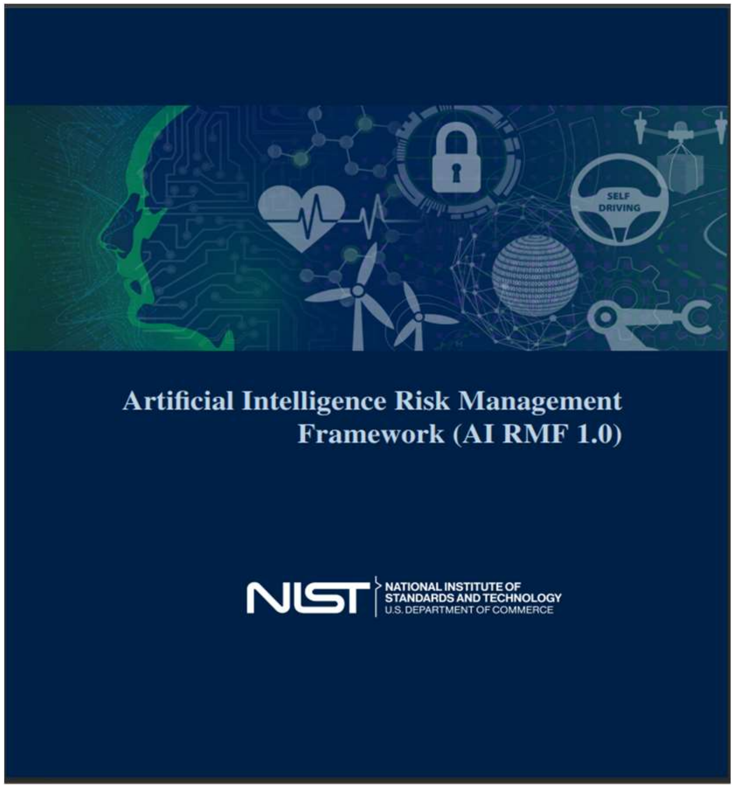
Harm to an Organization

- Harm to an organization's business operations.
- Harm to an organization from security breaches or monetary loss.
- Harm to an organization's reputation.

Harm to an Ecosystem

- Harm to interconnected and interdependent elements and resources.
- Harm to the global financial system, supply chain, or interrelated systems.
- Harm to natural resources, the environment, and planet.

Fig. 1. Examples of potential harms related to AI systems. Trustworthy AI systems and their responsible use can mitigate negative risks and contribute to benefits for people, organizations, and ecosystems.

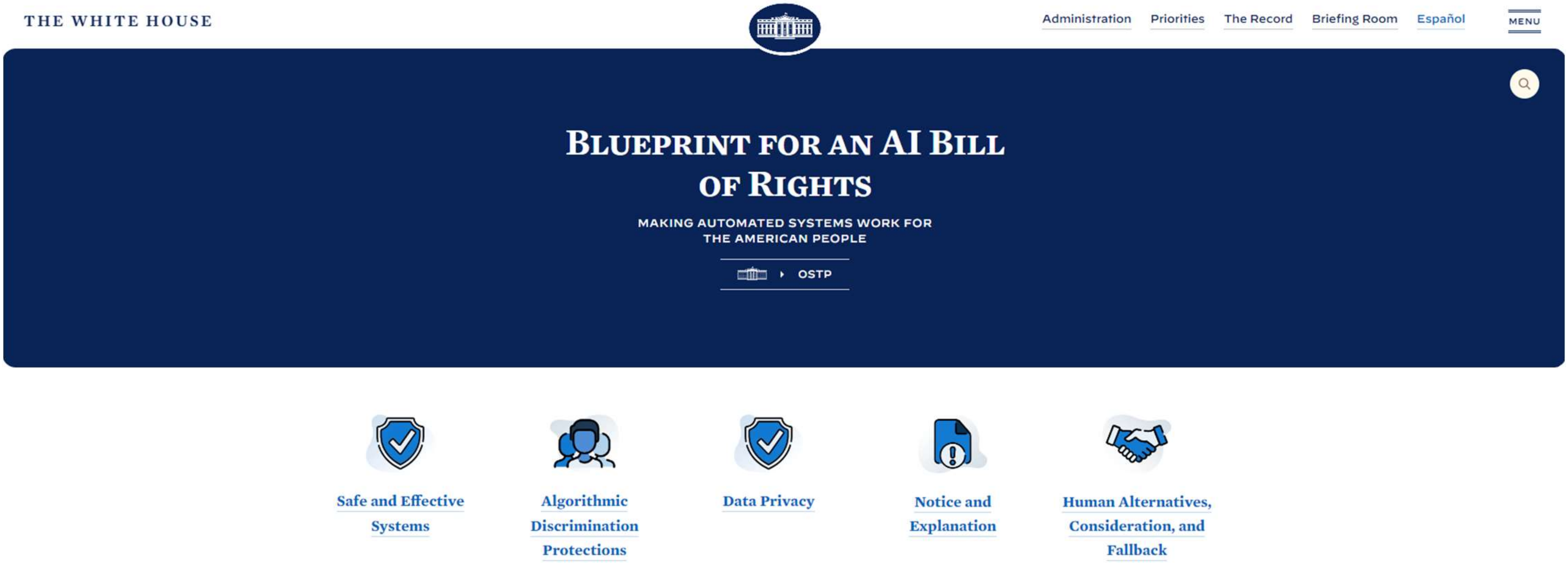


Artificial Intelligence Risk Management Framework (AI RMF 1.0)

NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE

https://nvlpubs.nist.gov/nistpubs/ai/NIST.AI.100-1.pdf

BILL OF RIGHTS



THE WHITE HOUSE

Administration Priorities The Record Briefing Room Español MENU

Blueprint for an AI Bill of Rights

MAKING AUTOMATED SYSTEMS WORK FOR THE AMERICAN PEOPLE

OSTP

Safe and Effective Systems

Algorithmic Discrimination Protections

Data Privacy

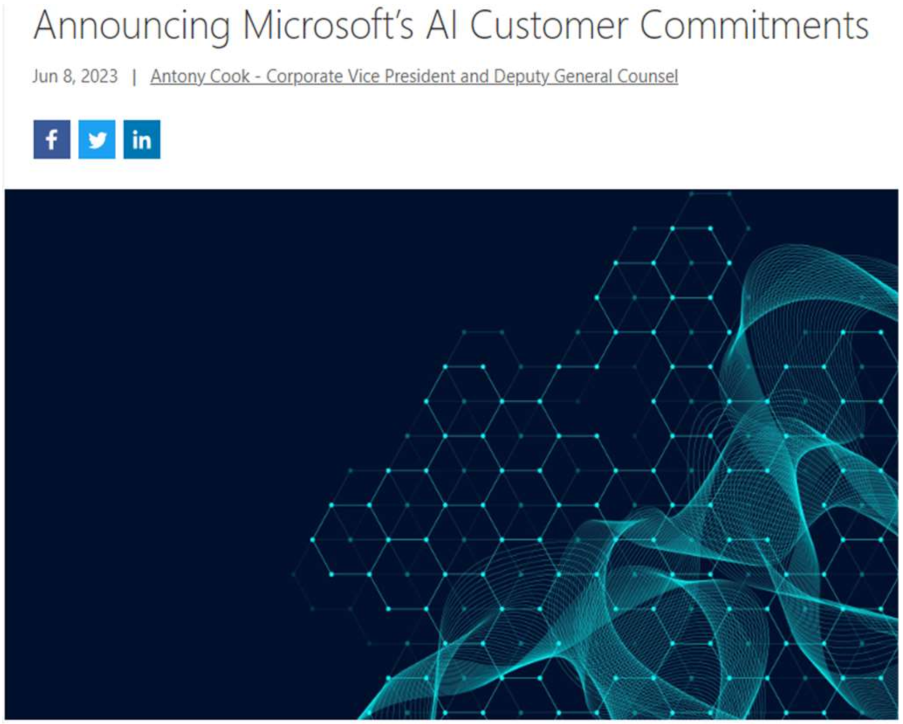
Notice and Explanation

Human Alternatives, Consideration, and Fallback

https://www.whitehouse.gov/ostp/ai-bill-of-rights/

AI GOVERNANCE POLICY

- Active involvement by leadership
- Scope of technologies covered
- Employee training
- Acceptable/ethical use
- Prohibited uses
- Transparency/Disclosure
- Oversight of AI usage
- Living document



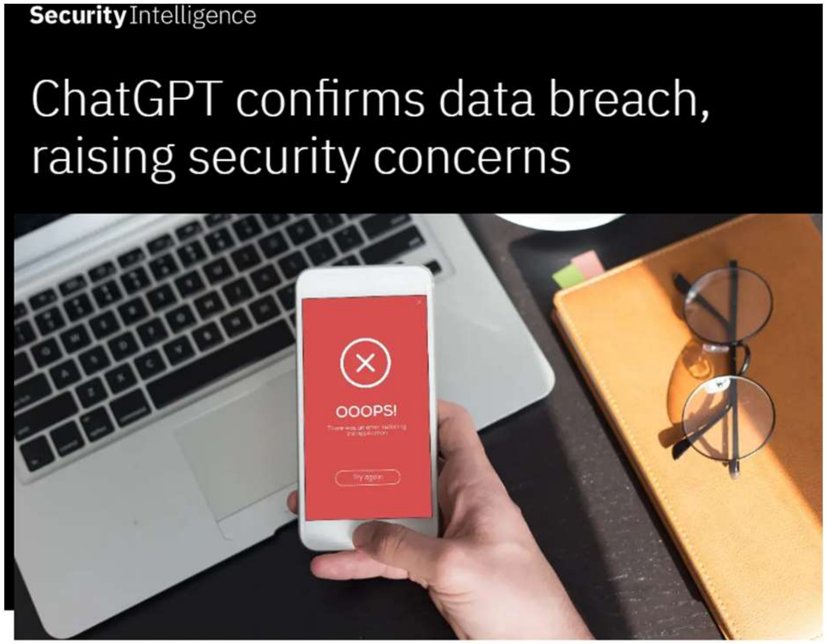
Announcing Microsoft's AI Customer Commitments

Jun 8, 2023 | Antony Cook - Corporate Vice President and Deputy General Counsel

https://blogs.microsoft.com/blog/2023/06/08/announcing-microsofts-ai-customer-commitments/

DATA PRIVACY/SECURITY

- Evaluation of AI tools
- Protection of data/confidentiality
- Access controls



Security Intelligence

ChatGPT confirms data breach, raising security concerns

https://securityintelligence.com/articles/chatgpt-confirms-data-breach/

QUESTIONS?

WOODS
ROGERS
VANDEVENTER
BLACK
ATTORNEYS AT LAW

Beth Burgin Waller
Chair, Cybersecurity & Data Privacy
beth.waller@wrvblaw.com

Jonathan V. Gallo
Cybersecurity & Data Privacy
jonathan.gallo@wrvblaw.com