K2’s Ethics And Privacy In AI

September 9, 2025

Tommy Stephens

CPA from Woodstock, Georgia

Partner, K2 Enterprises

Thirty-nine years public accounting & private industry experience

BSBA (Accounting) Auburn University

MS (Finance) Georgia State University

Please contact me: tommy@k2e.com

Follow me on X: @TommyStephens

Major Topics

Major provisions of AI security and privacy policies

Key risks associated with using AI tools

Steps to take to mitigate AI security and privacy risks

What Is Artificial Intelligence?

- Simply put, artificial intelligence (**AI**) uses computers to perform tasks that humans would perform otherwise
- Some examples of AI applications include machine learning (**ML**), speech recognition, and analyzing data for trends
- Notably, most who study the topic consider ML to be a subset of AI…further, almost every business professional uses ML, although many may not recognize that they use it
  - For example, adding rules to Outlook could be considered an example of ML

What Is ***Generative*** AI?

- Conceptually, generative AI is quite simple…it is a form of AI that allows technology to generate customized responses to your questions and prompts
- Recent advancements in Large Language Models (LLMs) allow generative AI tools such as **ChatGPT**, **Claude**, **Copilot**, **Gemini**, and others to create responses to your prompts
- Although not technically correct, it might be fair to think of generative AI tools as turbo-charged search engines

Generative AI Offers Many Options To Improve Your Productivity

Research

Writing

Analyzing data

Reducing email burdens

Creating PowerPoint presentations

Generating images

Sounds good…right?

SO, WHAT COULD POSSIBLY GO WRONG?

Plenty!

Biased Outputs

Copyright Infringement

Data Privacy

Data Security

Deepfakes

Hallucinations

Biased Outputs

- **Bias** in the context of AI refers to the situation where AI provides an incorrect answer because of the following issues
  a) Insufficient data in the language model on which to base a result
  b) Poor training of the data in the language model
  c) A combination of both the above factors
- Theoretically, bias could be intentional, but that is increasingly unlikely due to profit motives
  - AI platforms that provide unacceptably higher numbers of incorrect answers are not going to be as profitable as those that have higher accuracy rates

Copyright Infringement

Who owns the copyright to materials generated by AI?

In the United States, ***the Copyright Office has stated that it will not register works that were created by an autonomous AI tool****. This means that, under current US law, AI-generated works are either in the public domain or they are derivative works of the materials that the AI was trained on.*

Copyright Infringement

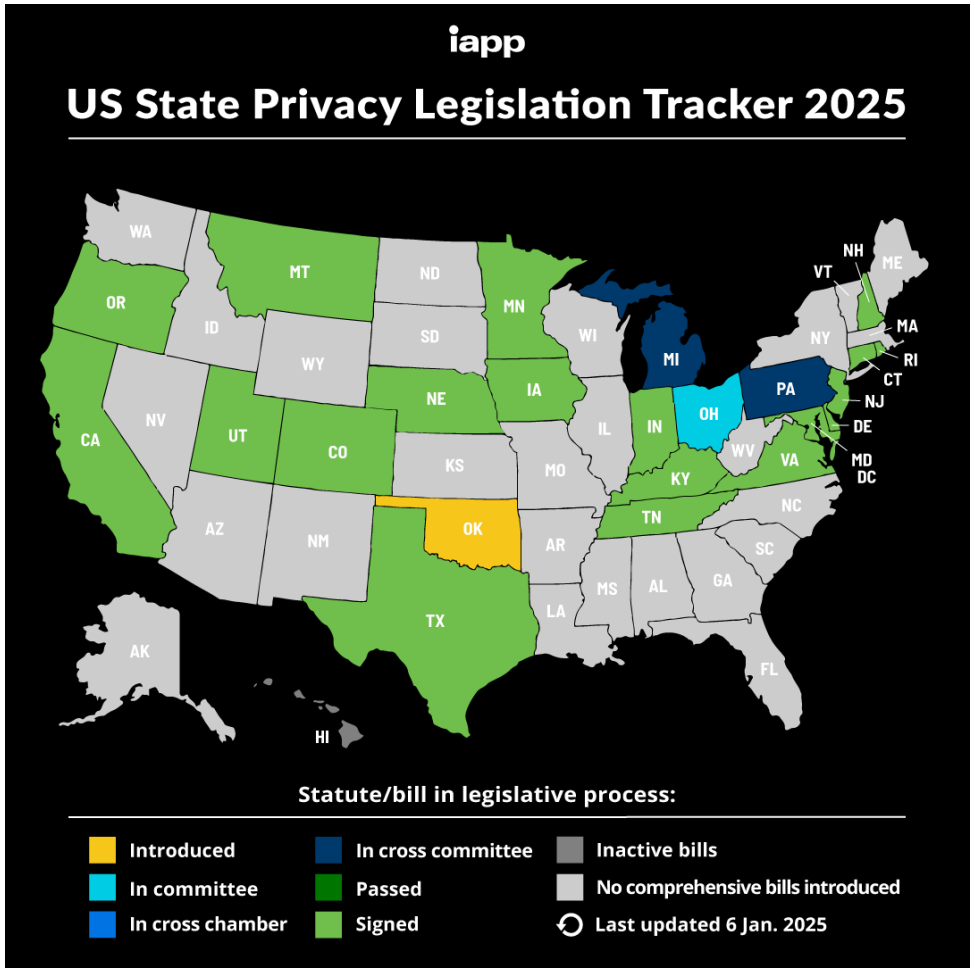
New York Times Has Sued MSFT & OpenAI!

- In December 2023, the New York Times sued Microsoft and ChatGPT's parent company, OpenAI
- The Times alleges "*mass copyright infringement*" related to ChatGPT allegedly publishing an article written by a NYT author without attribution and compensation
- The Times stated: *"These tools were built with and continue to use independent journalism and content that is only available because we and our peers reported, edited, and fact-checked it at high cost and with considerable expertise."*

Data Privacy

- Consider the type of data you might upload into an AI tool or platform…how comfortable are you that sensitive data remains private and not identifiable back to an individual, a client, or an organization?
- Other issues include
  - Is there informed consent about collection and use
  - The threat of exposing sensitive data through a breach or attack
  - Lack of transparency regarding using an individual's or organization's data

US State Privacy Legislation 2025



Data Security

- Like other large caches of data, the data stored in AI tools and platforms can present an inviting target because of the private nature of the data
- Additionally, a general lack of human oversight can increase the vulnerability of the data
- Moreover, the complexity of AI systems presents challenges concerning storing and protecting sensitive data
- In fact, as reported on 11/10/23, Microsoft temporarily blocked team members from using ChatGPT due to security concerns

Deepfakes

- Unscrupulous people can use AI to generate **deepfakes**
- Deepfakes are “synthetic” audio, visual, or audiovisual media clips that can depict real or fictional events
- Often, fictional deepfakes are used to embarrass an individual or to undermine a person’s credibility
- Because of the emergence of AI, today is quite easy to create a deepfake that appears to be “authentic”

Hallucinations

- An AI “hallucination” occurs when AI provides an incorrect answer for no explicable reason
  - Contrast that to bias, where we can identify the lack of data or the poor training
  - Two examples
    - In February 2023, Gemini incorrectly asserted that the Webb Space Telescope took the first image of a planet outside the solar system. In reality, the pictures of an exoplanet were taken in 2004
    - Several newspapers in the USA published a summer book list where the majority of the listed titles did not actually exist. These books, credited to real and reputable authors, were AI hallucinations

Understand what you're getting into with generative AI

SOFTWARE LICENSES AND PRIVACY POLICIES

Just Another Battle In A Long War…

- Historically, software licensing and use policies have been a problem for parties on both sides of the fence
- That hasn't changed with AI, and likely will not change soon
- **On the developer side, there is an incentive to get as much quality data as possible into the LLMs, while simultaneously building up the subscriber base**
- **However, on the end-user side, we should not share data that is private/sensitive with the outside world**
  - Do you ***really*** want to upload your tax return to an AI platform?

Add AI And It Gets Complicated

- Software licensing and data usage policies have always been hard to understand – even with search engines
- Now, consider the impact of Artificial Intelligence (AI) when added to the mix
- Could creating a prompt asking for tax advice expose your personal data or that of a client?
- Could uploading financial data for a privately-held company to an AI platform cause that data to leak?
- Can we trust what the AI companies are telling us about data security and privacy?

Understanding Licenses Is Critical

- To better understand the risks associated with privacy and AI, we need to **READ** and **UNDERSTAND** the major documents associated with the application
- Two of the key documents associated with your rights/license to use software or cloud-based services include:
  - End User License Agreement (EULA) a/k/a Terms of Service (ToS)
  - Privacy Policy

ChatGPT's Terms Of Use Key Points

- Must be at least 13 and, if under 18, have parental consent
- Cannot use ChatGPT for “illegal, harmful, or abusive” activity, including infringing upon or violating anyone’s rights
- You cannot represent that results are human-generated
- You retain ownership rights to your inputs and outputs
- ChatGPT can use your content to “provide, maintain, develop, and improve our services”
- You can opt out of ChatGPT using your data to train ChatGPT

https://openai.com/policies/terms-of-use/

What Data Is Used To Train LLMs

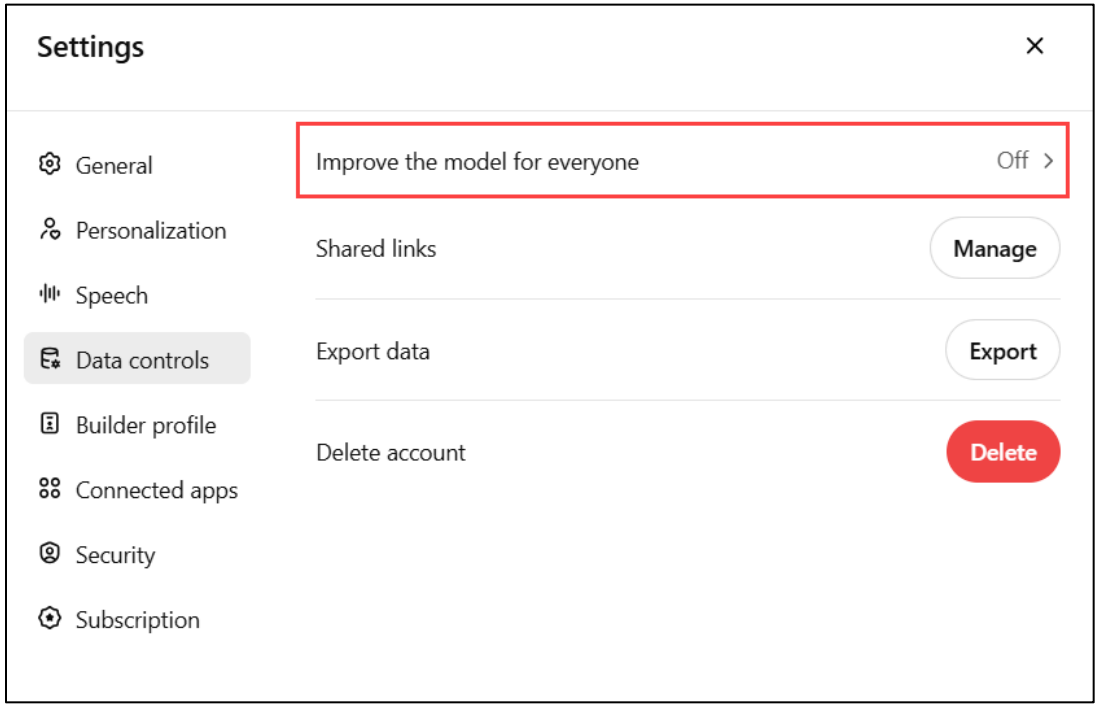
Information that is publicly available on the internet

Information that we partner with third parties to access and use

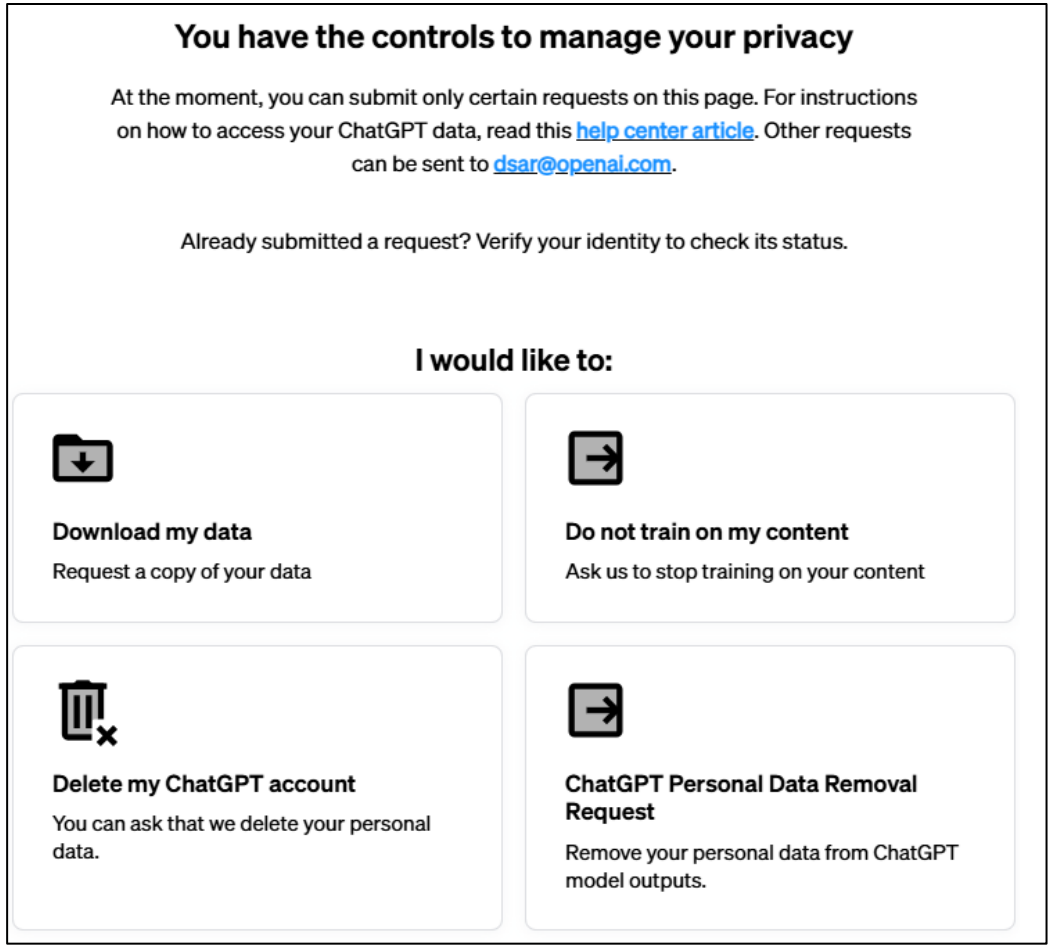
Information that our users or human trainers and researchers provide or generate

To Opt-Out Of ChatGPT's Training…

- Visit ChatGPT's **Settings**
- Next, click **Data controls**
- Finally, turn off the **Improve the model for everyone** option as shown on the right
- It's a good idea to review all the other settings also to ensure they align with your expectations and needs



ChatGPT’s Privacy Request Portal



- You can find the **Privacy Request Portal** at https://k2e.fyi/OAIPrivacy or by using the QR code below

Privacy Policy

- Document which discusses a company's privacy policy, including data like
  - What data is gathered from you
  - How your information will be used
  - The purpose of gathering that data and how your data may be used
  - When your data will be disclosed to others, including sensitive personal data and information
    - Not always specific on with whom it will be shared
  - Security policies and procedures
- Consider ChatGPT's Privacy Policy

Acceptable Use Policy

- Just as the EULA/ToS, and Privacy Policy spell out the rights and responsibilities of both parties in a relationship between an end user and a software company, an Acceptable Use Policy (AUP) governs the acceptable use of the organization's technology hardware, software, and data by its employees and contractors
- Although acceptable use policies are not required by law, they help both employees and companies properly set expectations about how these tools will be used (and how they will NOT be used) so all parties know their rights and responsibilities

Acceptable Use Policy Defines

- Ownership and general use of technology
- Security and handling confidential information
- Types of unacceptable use of systems
- E-mail and communication guidelines
- Blogging and social media
- Consequences for violation of these policies

Potential Harms From AI Systems

Source: "Artificial Intelligence Risk Management Framework" (AI 100.1) by US National Institutes for Standards and Technology (NIST)

SO, WHAT ARE THE AI COMPANIES SAYING?

ChatGPT Data Concerns

- OpenAI (ChatGPT's parent company) collects:
  - IP address, location, browser type, date/time, length of session, device name, and operating system
  - Uses cookies to track browsing activities both in chat window and site
  - Records complete transcripts of your prompts and conversations
  - ChatGPT reserves the right record any data you upload, such as an Excel file or a set of financial statements
- As discussed previously, to enhance security and privacy, consider opting out of model improvement and deleting your chat history

Gemini Concerns

- Google publicly stated that Gemini collects the following information about your use of Gemini
  - Conversations, locations, feedback, and usage info
- Regarding accessing to your Gemini conversations, Google says the following: *We take your privacy seriously, and we do not sell your personal information to anyone. To help Gemini improve while protecting your privacy, we select a subset of conversations and use automated tools to help remove user-identifying information (such as email addresses and phone numbers).*

Gemini Concerns

- Google goes on to state: *Please don't enter confidential information in your conversations or any data you wouldn't want a reviewer to see or Google to use to improve our products, services, and machine-learning technologies.*
- *Gemini Apps conversations that have been reviewed by human reviewers are not deleted when you delete your Gemini Apps activity because they are kept separately and are not connected to your Google Account. Instead, they are retained for up to three years.*

MICROSOFT'S COPILOT OFFERING IS A BIT DIFFERENT

Microsoft’s AI Copilots

Name	Products	Monthly Cost	Commercial Data Protection Included?
Copilot for MS 365 (Business/Enterprise)	Microsoft 365 apps (Word, Excel, PowerPoint, Outlook, Teams)	$30 per user	**Yes**
Copilot in Windows (Bing Chat)	Windows OS	Free	Not for home users, included with most business/enterprise O365/M365 plans
Copilot Pro for Individuals	Advanced features on top of standard Copilot, plus integration with home Microsoft 365 apps	$20/user/mo.	Not specified
Copilot for Security	Microsoft’s cybersecurity products	Consumption-based fee - $4/hour	Not specified
Copilot for Finance, Sales, and Service	Financial operations, sales optimizations, service enhancements	$50/user/mo., $20/user/mo. if already have MS 365	Not available to other customers, runs on Microsoft cloud in separate instance of ChatGPT, not used by MS to train models by default
Designer for Copilot	Image creation and editing	Not available	No
Copilot GPTs and Azure AI Studio	Custom generative AI assistants and solutions	Not specified	Not specified

Enterprise Data Protection

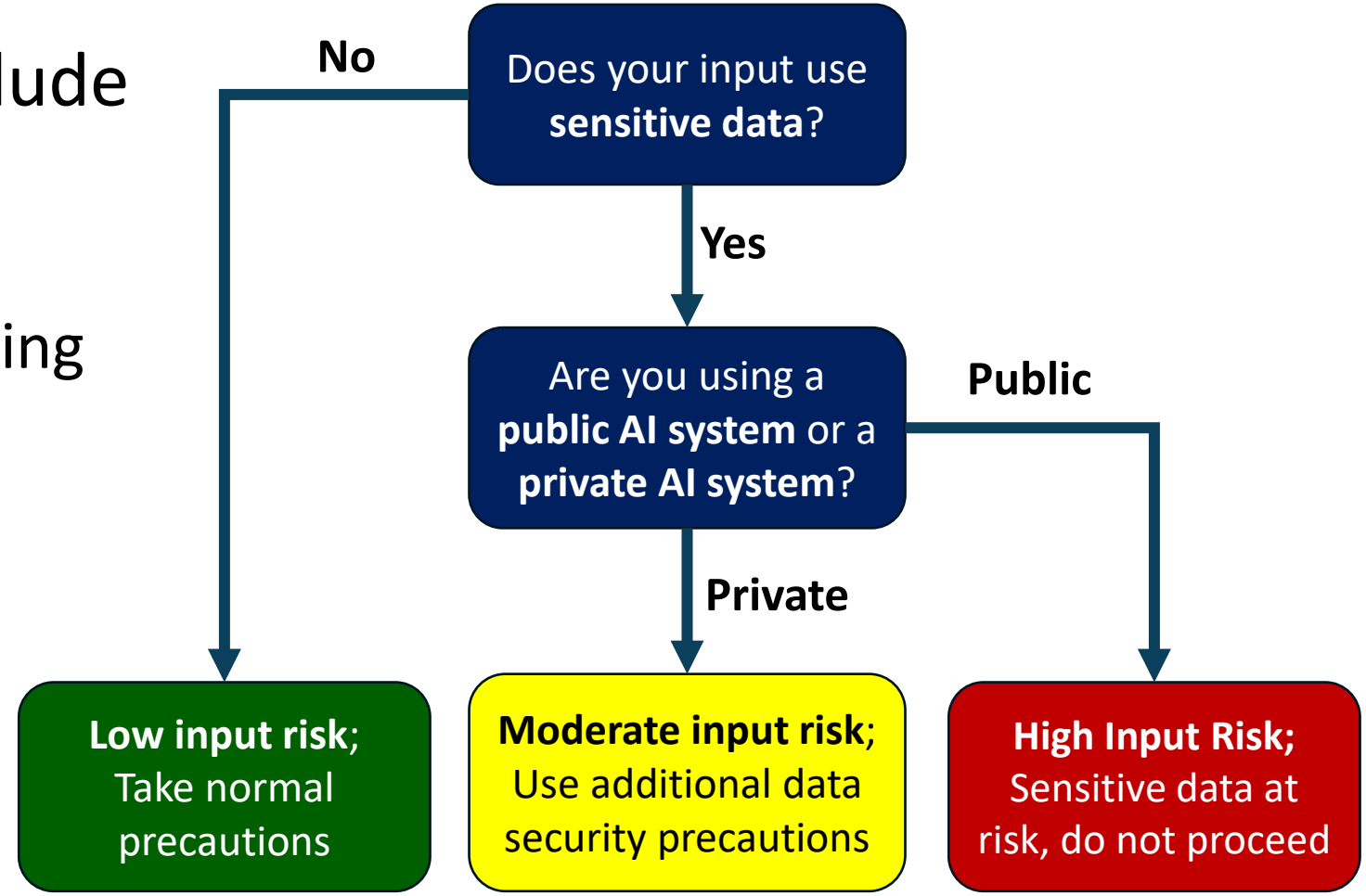
- **Authentication**: It uses Microsoft Entra ID to ensure only authorized users can access Copilot with commercial data protection
- **Data Encryption**: Chat data is encrypted both in transit and at rest using advanced encryption standards
- **Privacy**: Prompts and responses are not saved or used to train the underlying models//Microsoft has no “eyes-on” access to this data
- **Anonymity**: Search queries triggered by prompts are not linked to users or organizations
- **Ad Protection**: Advertising shown to users isn’t targeted based on their work identity or chat history

Three Types Of GenAI Risk

Input risks	Output risks	System risks
• The risks associated with exposing your proprietary data to an AI system and that data becoming compromised, which results in unauthorized disclosure of confidential information	• The risks that the outputs from the AI model will be low quality, inaccurate, or incomplete and the models lose their integrity based on including an unacceptable number of erroneous data points	• Risks associated with the servers hosting the AI system being compromised and the data model needs to be recovered from backups

Gen AI Input Risk Decision Tree

- Types of input attacks include attempts to:
  - Crash AI model
  - Exfiltrate memorized training data

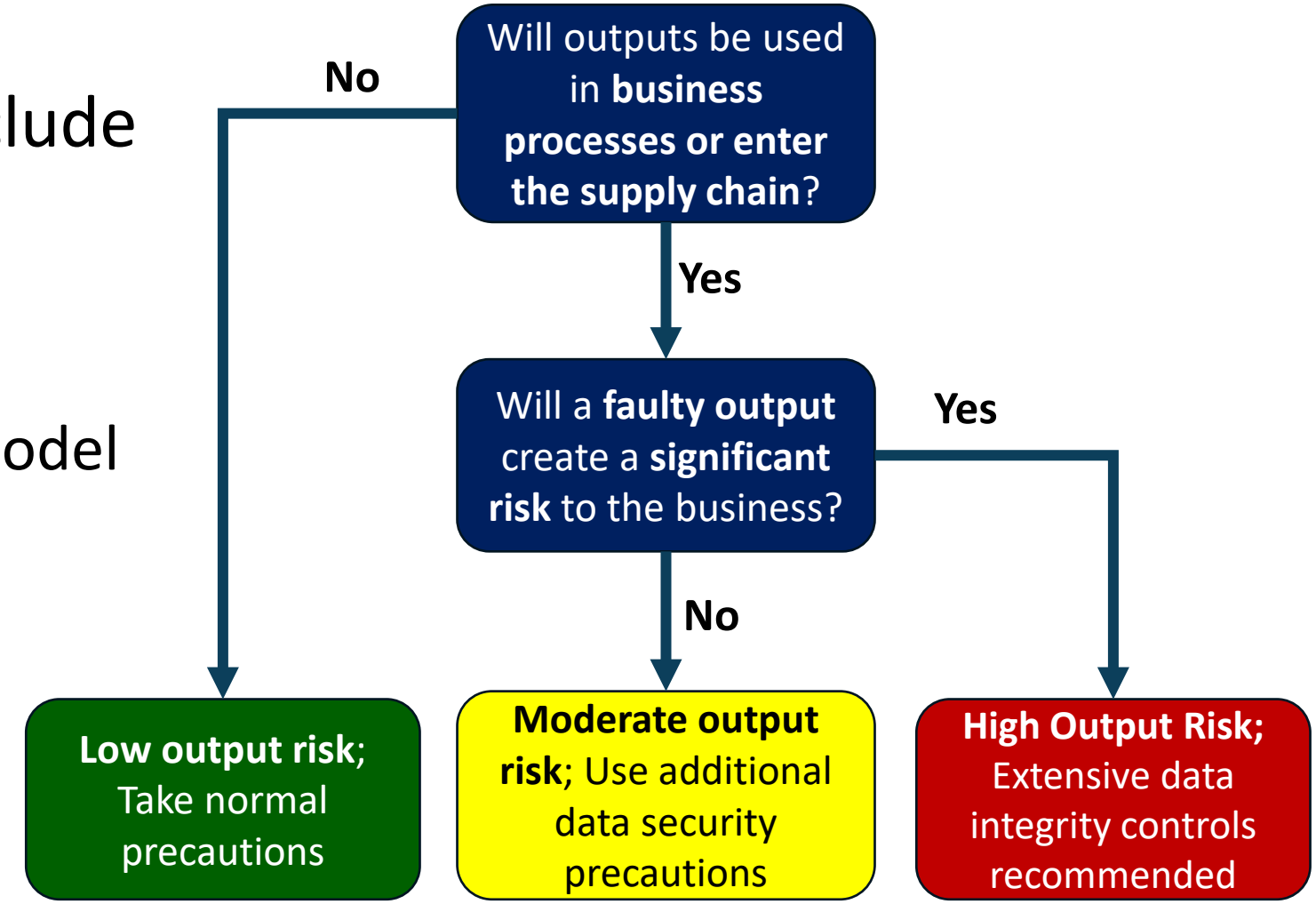


Source: "Address Security & Privacy Risks for Generative AI" by InfoTech Research Group

Gen AI Output Risk Decision Tree

Types of output attacks include attempts to

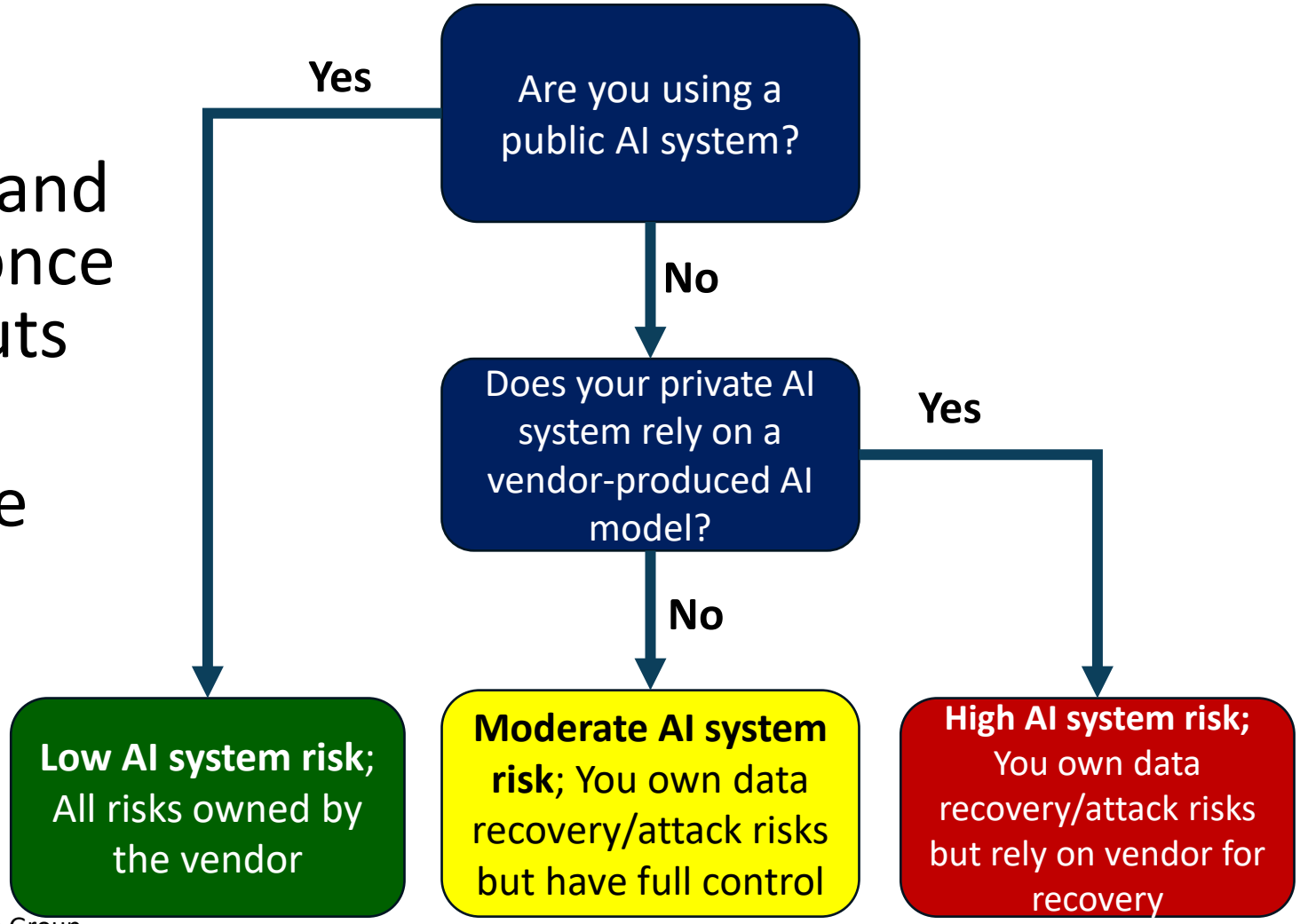
- Data poisoning that could corrupt AI output
- Weaponization of an AI model
- Sponging to slow down processing speed of AI model



Source: "Address Security & Privacy Risks for Generative AI" by InfoTech Research Group

Gen AI System Risk Decision Tree

- Public AI systems like ChatGPT, Google Gemini, and Bing chat are developed once and trained based on inputs from many users
- Private AI systems must be trained, managed, and maintained by employees using internal organization resources



Source: "Address Security & Privacy Risks for Generative AI" by InfoTech Research Group

Summary And Wrap Up

- Generative AI is here to stay, and it can be a wonderful addition to your set of business tools
- Using AI to become more productive and effective offers tremendous promise to all users!
- But, we must be careful when working with AI platforms so as not to allow any leakage of private data to outside parties
- Explore and take advantage of today's AI tools, but please exercise appropriate caution as you do so!

Summary And Wrap Up

- Proactively manage the security and privacy settings in the AI platforms that you use
- Never enter or upload private or sensitive data into your generative AI prompts
  - Scrub names, SSNs, account numbers, etc., from your data before uploading it to a generative AI tool
- Train your team members on how to use these tools safely and securely…remember the survival of your business may depend upon it!

tommy@k2e.com

THANKS FOR THE PRIVILEGE OF SHARING!

THANKS FOR JOINING ME TODAY!

The materials provided are for educational purposes only. The information presented is intended to assist in learning and should not be considered professional advice. While every effort has been made to ensure the accuracy and reliability of the content, the creator(s) and distributor(s) of this material do not assume any responsibility or liability for any errors, omissions, or consequences resulting from the use of this information. The views and opinions expressed in this material are those of the author(s) and do not necessarily reflect the views of any affiliated institutions or organizations. Additionally, Artificial Intelligence tools may have been used to assist with developing this content.

Privacy And Security Checklist For ChatGPT

APPENDIX

ChatGPT’s Privacy & Security Checklist

- **Account & Access Security**
  - Use a strong, unique password for your Open AI account
  - Enable two-factor authentication
  - Avoid shared accounts
  - Sign out after each session on a shared computer
  - Limit access device and use only trusted, secure devices

- Per ChatGPT’s website at https://chatgpt.com/c/68713cf9-61e0-800d-8739-042730793f59

ChatGPT’s Privacy & Security Checklist

- **Data Sensitivity And Input Controls**
  - Avoid entering sensitive personal information such as Social Security Numbers or financial account numbers
  - Do not upload confidential business documents unless anonymized or authorized
  - Redact client information from all prompts before sharing
  - Avoid discussing or inputting proprietary code or trade secrets

- Per ChatGPT’s website at https://chatgpt.com/c/68713cf9-61e0-800d-8739-042730793f59

ChatGPT’s Privacy & Security Checklist

- **Chat & Data Settings**
  - Turn off chat history if you do not want your prompts saved or used to improve the model
  - Delete old chats that contain sensitive content
  - Review and clear your data regularly using the “Manage My Data” option in your account settings

- Per ChatGPT’s website at https://chatgpt.com/c/68713cf9-61e0-800d-8739-042730793f59

ChatGPT’s Privacy & Security Checklist

- **Enterprise and Professional Use**
  - Use ChatGPT Team or Enterprise for additional security and control
  - Ensure that your organization’s data usage policies allow for the use of generative AI tools such as ChatGPT
  - Review OpenAI’s data usage policies and TOS to understand what is stored and what is deleted

- Per ChatGPT’s website at https://chatgpt.com/c/68713cf9-61e0-800d-8739-042730793f59

ChatGPT’s Privacy & Security Checklist

- **Secure Network Practices**
  - Use a VPN when accessing ChatGPT on public WiFi
  - Ensure your browser is up-to-date with the latest security patches
  - Enable HTTPS-only mode in your browser setting for encrypted connections

- Per ChatGPT’s website at https://chatgpt.com/c/68713cf9-61e0-800d-8739-042730793f59

ChatGPT’s Privacy & Security Checklist

- **User Awareness And Best Practices**
  - Treat ChatGPT like a public forum – assume others could access your inputs unless using an enterprise-secure environment
  - Never rely solely on AI for sensitive decisions without human oversight
  - Train team members on responsible AI use and data privacy protocols
  - Periodically review audit trails or logs (if using enterprise tools) for unexpected access or activity

- Per ChatGPT’s website at https://chatgpt.com/c/68713cf9-61e0-800d-8739-042730793f59