GENERATIVE AI TOOLS: PRIVACY RISKS, APPLICABLE LAWS AND PRACTICAL COMPLIANCE

NOVEMBER 2023

orrick

What Is It?

- Machine learning models designed to generate new content in the form of text (including code), audio, images, video
- Receives input instructions or "prompts" (text or A/V) to guide content creation
- Produces new content as "outputs" or "suggestions"
- Types of Models
  - Large Language Models (LLMs)
  - Diffusion Models

Stable Diffusion - “Patent Figure of a Flying Bicycle”

THE GENERATIVE AI REVOLUTION

How Is It Used?

Example Use Case	The Good	The Bad
Email Drafting & Automated Response	Automate responses to common employee / customer questions, and reduce time spent on email creation	Generate sophisticated and personalized phishing campaigns with limited to no resource barriers
Voice Recordings & Chatbots	Quickly create and adjust realistic voice prompts without employee or voice actor involvement	Generate convincing messages or chatbots impersonating persons of authority to gain trust or access
Image & Video Personalization	Develop personalized business images and videos without diverting employee time or hiring models	Generate realistic but fake visual content to damage reputation or carry out blackmail
Code Development & Testing	Rapidly generate code for new software use cases, and automatically detect and correct bugs	Generate look-alike malware capable of evading traditional signature-based detection measures

RISKS OF USING GENERATIVE AI

Exposure of Confidential Information / Trade Secrets

- AI Inputs can include short text, lengthy documents, images
- Many AI tools provide for licensed reuse of prompts and other inputs for retraining of model and ongoing service development
- Employees are using AI tools without employer knowledge

DIVE BRIEF

Most employees using ChatGPT, other AI tools for work aren't telling their bosses

Published Feb. 7, 2023

RISKS OF USING GENERATIVE AI

Inappropriate Outputs & Generated Content

Hallucinations & Misinformation

AI model generates outputs that are completely or partially incorrect, unrealistic, or inconsistent with the input or desired output.

Causes include:

- Model trained on insufficient data
- Model asked to perform task for which it is not well-suited
- Model encounters data differing significantly from training data

Bias, Discrimination & Harmful Content

AI model generates outputs that reflect inherit biases or harmful content contained in the data on which they are trained.

Examples include:

- Gender biases in generated text (e.g., masculine pronouns)
- Inaccurate portrayal of minorities in generated images
- Aggressive language in conversational chats

Infringing Content

AI model generates outputs that infringe on a third party's rights. Company may not be aware of potential infringement.

Examples include:

- Patent infringement
- Copyright infringement
- Trademark infringement (product, logo, packaging)
- Synthetic media infringement (voice/likeness)

RISKS OF USING GENERATIVE AI

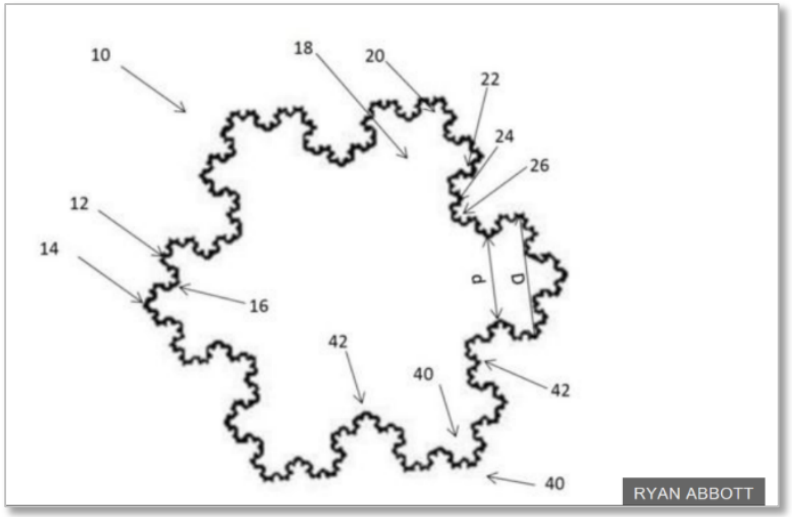
Uncertain Ownership: Copyright Protection

- *A Recent Entrance to Paradise*
- Copyright Office: AI cannot be a copyright author
- Copyright Office Guidance 3/16/23
  - applicants have a duty to disclose the inclusion of AI-generated content in works submitted for registration
  - disclaimer versus seeking protection for AI-assisted outputs

RISKS OF USING GENERATIVE AI

Uncertain Ownership: Patent Protection

- Law requires a human inventor for patent protection
  - *Thaler*
  - Dabus "invention" rejected by USPTO, UK, and EU
- Nature of conception need not be disclosed in an application. Section 103 expressly states that the way an invention was made is not relevant to obviousness.



- How much from a human is enough?
  - an inventor need only contribute to the conception of the invention
- USPTO Request for Comments 2/14/23

RISKS OF USING GENERATIVE AI

Uncertain Ownership: Patent Protection

- Under current law, not enough to qualify as an "inventor":
  - Doing experiments to test the invention
  - Reducing the invention to practice at the direction of the inventor
  - Setting design goals
  - Managing the inventors
  - Proposing obvious additions to the invention
  - Funding the work
  - Encouraging the inventors

Privacy Risks

- Privacy notice commitments and "processor" terms may restrict the ability to use personal data to train Generative AI or create generative content
- Sharing personal data with Generative AI vendors may constitute a "sale" necessitating the offering of the right to opt-out
- Processing personal data in new ways through Generative AI may result in new "purposes of processing" triggering purpose limitation restrictions
- Data previously considered "anonymized" or "pseudonymized" may be at a higher risk of reidentification within Generative AI
- Outputs resembling data subjects or stating "facts" about data subjects may be perceived as being invasive of individuals' privacy

RISKS OF USING GENERATIVE AI

Security Risks

- Integration of unproven Generative AI tools into company systems may create new vulnerabilities
  - Employees downloading tools / plug-ins to improve productivity without proper vetting
- Sophisticated phishing email generation with a higher probability of evading spam / malicious filters
- Life-like imitations with a greater capacity for gaining employee trust and bypassing advanced security measures (like voice detection)
- Increase in new malware and brute force attacks on traditional systems
- Adversarial attacks on Generative AI models themselves

RISKS OF USING GENERATIVE AI

Other Risk Examples

- Claims of consumer deception for lack of transparency regarding AI use
- Overstatement of benefits of AI in investor relations materials
- Inaccuracies in reports / financials produced using Generative AI
- Fake content / profiles bolstering company valuations
- Allegations of "market manipulation" from generated content
- Increased focus on data and AI technology ownership in antitrust
- Perceived discriminatory outcomes from labor adjustments

RISKS OF USING GENERATIVE AI

Evolving Laws & Ethics

time to press the pause button on generative AI development?

TECH · A.I.

Bill Gates opposes Elon Musk's call to pause new A.I. research because of what 'bad guys' could do

Artificial intelligence (AI)

AI 'could be as transformative as Industrial Revolution'

AI is moving fast. Washington is not.

Is DC doomed to make the same mistakes with AI that it made with social media?

AI

EU lawmakers eye tiered approach to regulating generative AI

Alarmed tech leaders call for AI research pause

As systems dazzle, researchers worry about lack of safeguards and regulation

AI needs superintelligent regulation

Effective brakes can help the industry move faster

AI Act: a step closer to the first rules on Artificial Intelligence

Big Tech cuts AI ethics teams even as development ramps up

Lina Khan: We Must Regulate A.I. Here's How.

Risk Mitigation Strategies

- **Awareness**
  - Understanding how the technology works, what tools are out there, how people are using them, and what lawmakers / regulators are doing in response is essential for predicting and addressing risks.
  - Trainings / working group sessions can help inform employees at all levels of the organization, and help avoid preventable harms (e.g., prompt-based risks, unapproved tool use).
- **Governance**
  - Designate diverse, cross-discipline group(s) responsible for developing and overseeing proper use of AI across the organization.
  - Identify AI champions within departments and teams who are passionate about the field to be the first point of contact for new policies, processes and tools.
  - Build in flexibility to address evolving technology, law and ethics.

Risk Mitigation Strategies

- **Policy**
  - Develop a Generative AI Responsible Use Policy outlining the company's position and guardrails for the use of Generative AI, including:
    - Ability to use Generative AI content outside of the organization
    - Restriction on using or generating confidential business information or personal data
    - Responsibility for human oversight and review of content for accuracy, quality, suitability, and standards
  - Update existing policies and procedures to address Generative AI risks, for example:
    - Investor Relations Guidelines on Generative AI Use and Statements
    - Restrictions on Use of Confidential Business Information with Generative AI
    - Privacy Impact Assessments for Generative AI Using / Producing Personal Data
    - Identification of Approval Workflows for External Distribution of Generative AI Content
    - Supplementation of Vendor Risk Management Program to Address AI Concerns

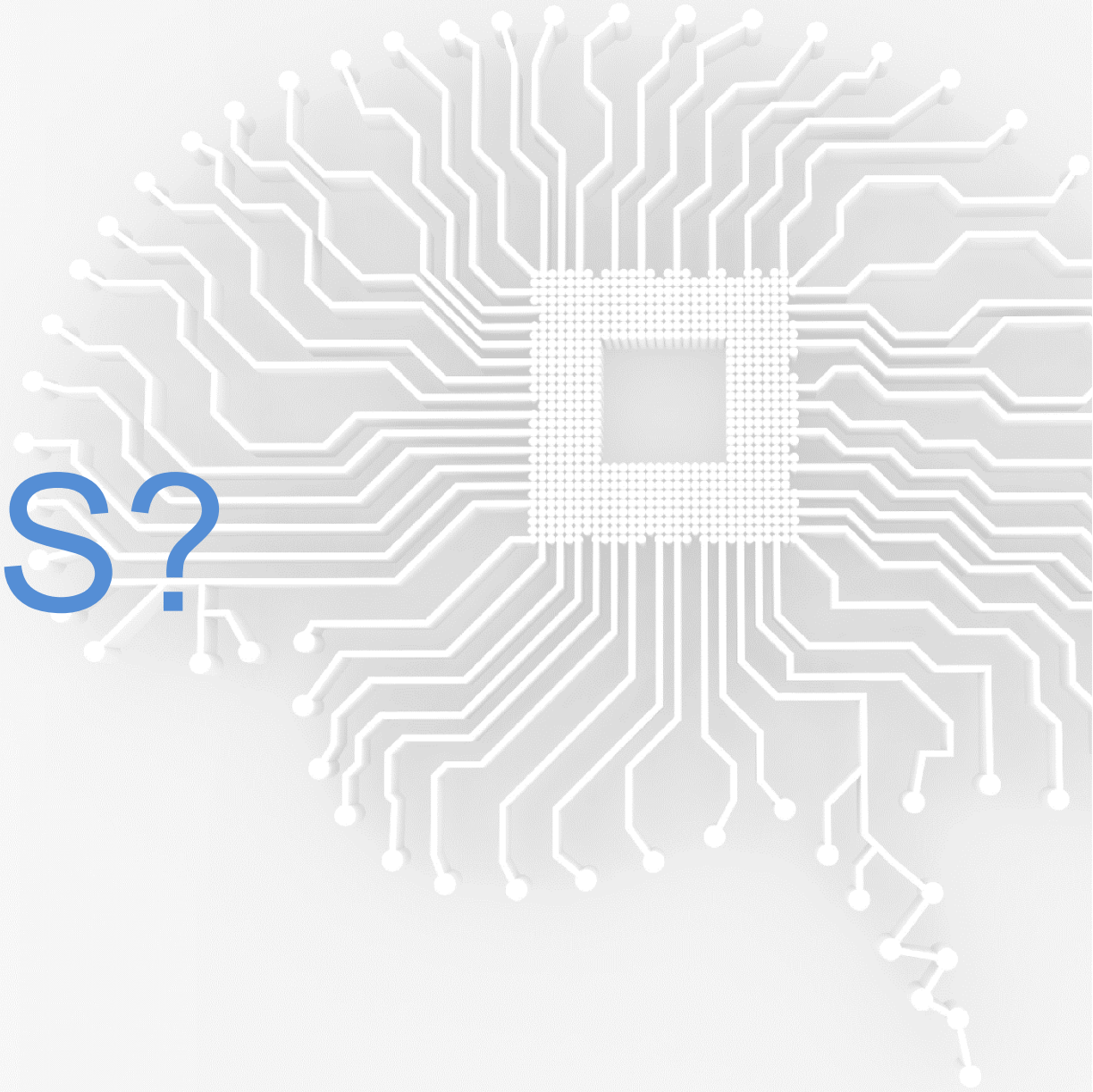
Risk Mitigation Strategies

- **Ownership Strategy**
  - Determine whether to build or buy relevant technology.
  - Consider use cases for assessment of acceptable risk to ownership of AI-assisted content creation.
    - Distinguish between peripheral and core of business operations.
    - Distinguish between peripheral and core functionality in products and services.
    - Consider outright prohibition for uses in core of business operations where IP ownership is essential.
      - Special considerations for source code
    - Consider use of services built on licensed datasets where IP ownership is important or risk tolerance for freedom to operate issues is low.
  - Confirm ownership of AI generated content under TOS; evaluate license-back terms; update CIIAA.
  - Incorporate human authorship (storyboard; complex prompts; iterate; edit) and audit trail.

Risk Mitigation Strategies

- **Diligence**
  - Gain an understanding of each tool's technology, use cases, strengths/flaws, and roadmap.
  - Scrutinize reuse of data and external tool connections.
  - Pilot new technologies prior to organization-wide roll outs.
  - Periodically test models to confirm they are operating as expected.
- **Contracting**
  - Scrutinize IP ownership provisions carefully to ensure they align with ownership strategy.
  - Ensure parties' rights and intended actions align with "controller" / "processor" designations.
  - Allocate liability for damages caused by technology vs. use appropriately.

QUESTIONS?



orrick