GUNDERSON DETTMER

DATA PRIVACY GROUP

Generative AI:

Navigating Privacy and Security Concerns in the U.S., EU and UK

April 26, 2023

Meet the Presenters

Anna Westfelt

Partner @ Gunderson Dettmer

Data Privacy

Frida Alim

Associate @ Gunderson Dettmer

Data Privacy

John Buyers

Partner @ Osborne Clarke

Commercial Practice
AI/ML Team

Gunderson AI Trainings

Presentation Series on Generative AI

Upcoming Webinars

Please look out for an invitation to these upcoming presentations:

Preparing for M&A Diligence

Best practices and guidance to prepare for the purchase or sale of AI companies or related assets.

Open Source Compliance

Open source issues and risks associated with using generative AI tools, including practical steps for incorporation and use of new technologies.

Prior Webinars

Regulating AI in Employment: *How to Comply and Best Practices Webinar*

Labor and employment best practices to comply with current and anticipated regulations governing automated decision making technology | LINK

Generative AI Developments: *Latest Developments, Legal Risks and Best Practices*

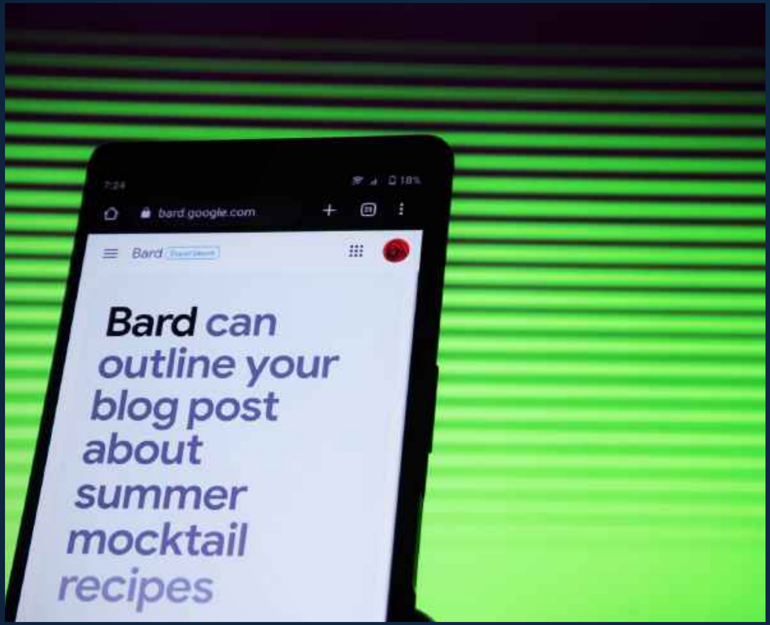
Covers developments in the AI landscape, including potential risks associated with AI, the recent case law updates, and methods for mitigating risks | LINK

Patenting AI: *What does it mean, should we do it, and what does success look like?*

Examines various aspects of AI that patents can protect, such as data preparation, training processes, and functional applications of AI | LINK

Generative AI Technology

Generative AI is a type of AI that uses machine learning algorithms to create new and original content.


bard.google.com
Bard
Bard can outline your blog post about summer mocktail recipes

Text

Generative AI can be used to write articles, scripts and poems.

Images

Generative AI can create new images based on existing ones, such as creating a portrait from a picture of a person's face, or an image from a description.

Sound

Generative AI can generate new music tracks, sound effects and voices.

GUNDERSON DETTMER

Agenda

1 | **U.S. Legal Landscape**

2 | EU/UK Legal Landscape

3 | Privacy Risks and Concerns

4 | Cybersecurity and Confidentiality

5 | Practical Tips and Panel Discussion

U.S. Legal Landscape

Regulation and Enforcement

- **State and Local Level**
  - State Privacy Laws regulating Automated Decision Making
  - California's AI Law? AB 331
  - Laws regulating employer use of AI (NYC Local Law 144, IL 820 ILCS 42, MD Lab. & Empl. § 3-717)
- **Federal Level**
  - American Data and Privacy Protection Act - *not passed*
  - Algorithmic Accountability Act - *not passed*
  - Blueprint for an AI Bill of Rights - *not passed*
  - FTC Rulemaking and Enforcement Actions

Agenda

1 | U.S. Legal Landscape

2 | **EU/UK Legal Landscape**

3 | Privacy Risks and Concerns

4 | Cybersecurity and Confidentiality

5 | Practical Tips and Panel Discussion

GUNDERSON DETTMER

EU/UK Legal Landscape

Regulation and Enforcement

- **GDPR (UK and the EU)**
  - "*Personally Identifiable Information*"
  - Accuracy
  - Lawful basis - consent vs. legitimate interests
  - "*Automated Decision Making*" (Article 22)
  - Data Protection Impact Assessments (DPIA)
- **EU Artificial Intelligence Act**
  - Top-down unitary framework
  - "*High Risk*" AI - specific use cases
  - "*Fundamental Rights*" Impact Assessments
  - Current progress in EU Parliament
- **EU AI Liability Directive**
- **UK AI Governance Framework**
- **Privacy-related enforcement and actions (GDPR based)**
  - Italian regulatory action
  - Other EU investigations - Spain, France, Germany, Ireland
  - UK regulator view

GUNDERSON DETTMER

Agenda

1 | U.S. Legal Landscape

2 | EU/UK Legal Landscape

3 | **Privacy Risks and Concerns**

4 | Cybersecurity and Confidentiality

5 | Practical Tips and Panel Discussion

Privacy Risks and Concerns

Internal Use of Generative AI

What are the privacy concerns with internal use of generative AI technology?

1 **Risks where Company trains a generative AI model**

Personal data contained in training data may be surfaced as an output

Establishing a lawful basis for processing personal data

2 **Risks where Company uses a third-party model that is fine-tuned using prompts**

Personal data contained in prompt may be surfaced as an output

3 **Disclosure of personal data to a third-party generative AI service may be considered a "sale" under certain Privacy Laws**

4 **Challenges associated with complying with data subject requests**

5 **Use of generative AI may trigger laws around Automated Decision Making, such as laws concerning profiling and automation in employment**

Privacy Risks and Concerns

Use of Generative AI in Products or Services

What are the privacy concerns with incorporating or using generative AI technology <u>in company products or services</u>?

1 | Personal data contained in inputs or other training data may be surfaced in outputs

2 | Issues associated with establishing a legal basis for training generative AI models using personal data

3 | Outputs made by generative AI may be inaccurate ("hallucinations")

4 | Issues regarding transparency of and justification for algorithm

Agenda

1 | U.S. Legal Landscape

2 | EU/UK Legal Landscape

3 | Privacy Risks and Concerns

4 | **Cybersecurity and Confidentiality**

5 | Practical Tips and Panel Discussion

Cybersecurity and Confidentiality

- ***Data exposure and loss***
  - Confidential information leakage (e.g., Samsung, Amazon)
  - Exposure of your code and vulnerabilities
  - Personal information
- ***Third-party code and threat actors***
  - Ingestion of third-party code and malicious elements/vulnerabilities
  - Social engineering attacks (e.g., phishing, deepfakes, voice impersonation, etc.)
- ***Can generative AI tools be used to improve cybersecurity?***
  - Potential use cases (e.g., malware analysis, drafting risk management policies, etc.)
- ***Role of the CISO***

Agenda

1 | U.S. Legal Landscape

2 | EU/UK Legal Landscape

3 | Privacy Risks and Concerns

4 | Cybersecurity and Confidentiality

5 | **Practical Tips and Panel Discussion**

GUNDERSON DETTMER

Practical Tips and Panel Discussion

Practical Steps To Consider Now

- **Internal use of generative AI**
  - ***Employee use*** - develop internal policy, implement employee training, internal monitoring and other guardrails
  - ***Organization use*** - compliance with regulated uses, including conducting third-party audits, DPIAs, etc.
- **Product use of generative AI**
  - OpenAI opt-outs and opt-ins
  - Microsoft Azure OpenAI Service
  - DPIAs or other conformity/impact assessments
- **Vendor management**
  - Onboarding and monitoring
  - Contractual considerations
- **Update public-facing terms and customer contracts**

Panel Discussion

MCLE Codes

- 1092
- 6436

We want your feedback!

Please email us at *insights@gunder.com*

GUNDERSON DETTMER