



Knobbe **Martens**

## **Protect and Respect: Legal Protections for Medical Devices & Data**

February 5, 2024

**Curtis Huffmire**

8<sup>th</sup> Annual Biomed Symposium

Irvine, CA

## Overview

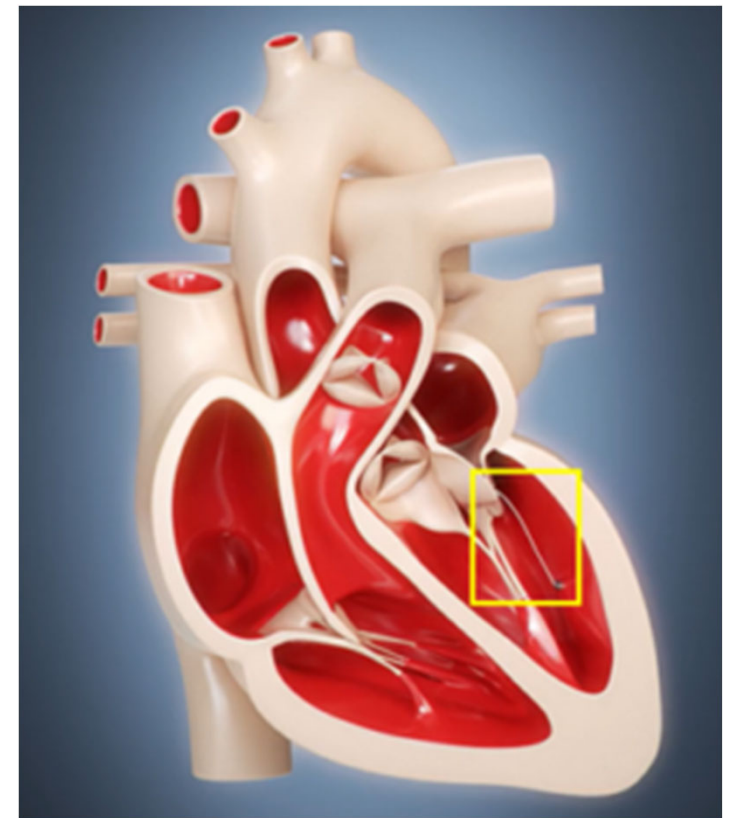
---

- Recent News and Deals in the in the Bio/MedTech Space
- Increasing Value by focusing on IP, Data Protection, and AI
- Protecting Innovation with Patents and other IP
- Respecting Privacy and Implementing Data Controls
- IP Developments related to Generative AI

# Recent News and Deals in the in the Bio/MedTech Space

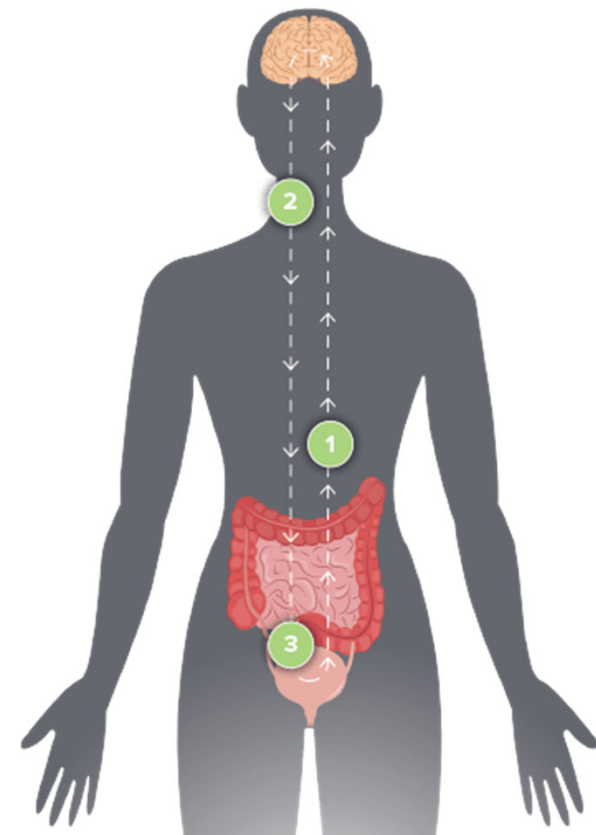
## Recent News and Deals in the in the Bio/MedTech Space

- CardioMech Raises \$13 Million for Transcatheter Mitral Chordal Repair
  - Norwegian clinical-stage company that treats mitral regurgitation using an artificial chord that extends between a flap of the mitral valve and a wall of the left ventricle.
  - With its Series A financing of \$18.5 in 2020, it has now secured total funding of \$42 Million.



## Recent News and Deals in the in the Bio/MedTech Space

- Boston Scientific to Acquire Axonics for \$3.7 Billion
  - Axonics, an Irvine urology company, uses a miniature implant to provide gentle stimulation to the nerves that control the bladder and bowel.
  - This can help restore normal communication between the brain and the bladder and bowel, which can improve symptoms associated with overactive bladder, fecal incontinence, or urinary retention.



## Recent News and Deals in the in the Bio/MedTech Space

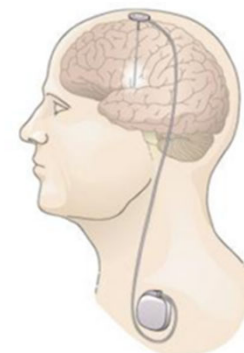
---

- Natera Gets \$96 Million Patent Infringement Verdict against CareDx and a Preliminary Injunction against NeoGenomics
  - Natera, a Texas company, has more than 400 issued or pending patents across organ health, oncology and women's health.
  - In a Delaware case, the jury awarded Natera \$83.7 Million in lost profits and \$12.6 Million in past royalties for patent infringement related to CareDx tests for detection of kidney transplant injury.
  - In a North Carolina case, Natera's MRD medical assay test, Signatera, and NeoGenomics' competing assay, RaDaR, are the only two tumor informed MRD tests on the market and are used for detecting trace amounts of circulating tumor DNA in patients, which can be used for early detection of cancer relapse. The district court found that Natera showed (1) it is likely to succeed on the merits, (2) it is likely to suffer irreparable harm in the absence of preliminary relief, (3) the balance of equities tips in its favor, and (4) an injunction is in the public interest.



## Recent News and Deals in the in the Bio/MedTech Space

- Deep Brain Stimulation Device Market to Reach \$3.5 Billion by 2033
  - DBS systems can be used for treatment of Parkinson's disease and other movement disorders. They can include a device that sends electrical signals through wire electrodes implanted in the brain.
  - A recent paper by market.us projects that the DBS devices market will grow from an expected \$1.5 Billion in 2024 to \$3.5 Billion by 2033.
  - Products in the DBS market include Abbott Labs' Liberta RC, an implantable and rechargeable pulse generator that recently received FDA approval and can receive and adjust therapy remotely, as well as Medtronic's Percept RC, also with FDA approval and touted as the thinnest dual channel neurostimulator on the market.



© 2024 Knobbe Martens

# Medtronic

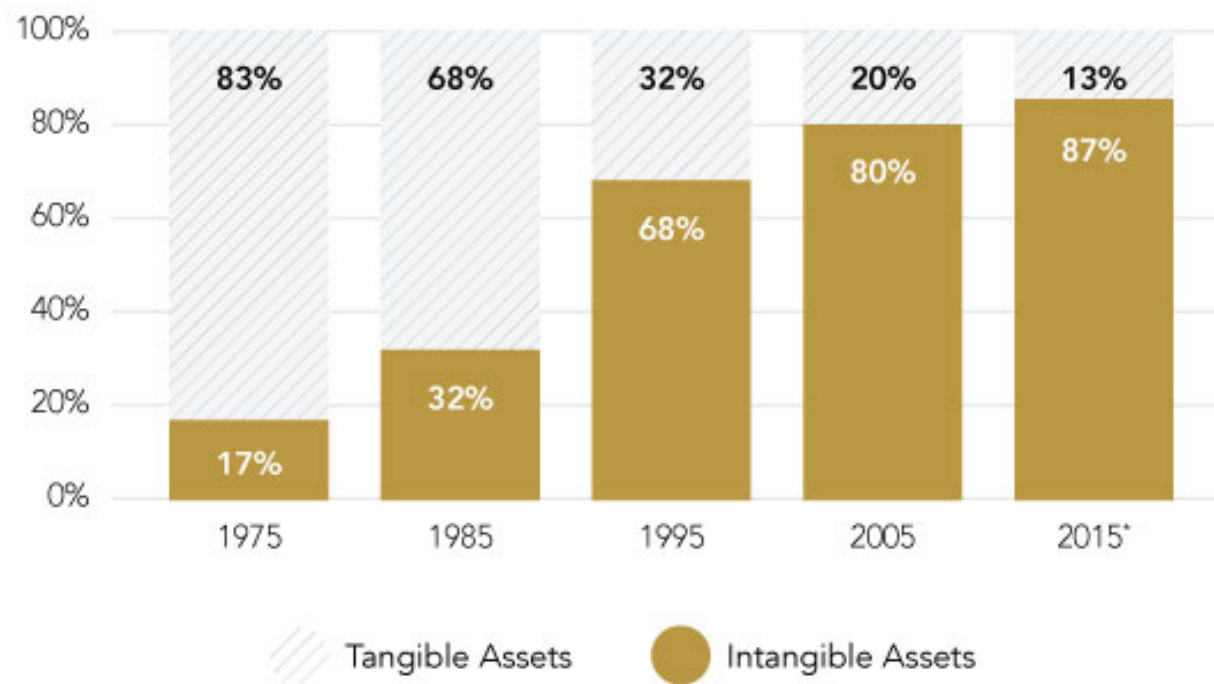


Increasing Value by focusing on IP, Data Protection, and AI

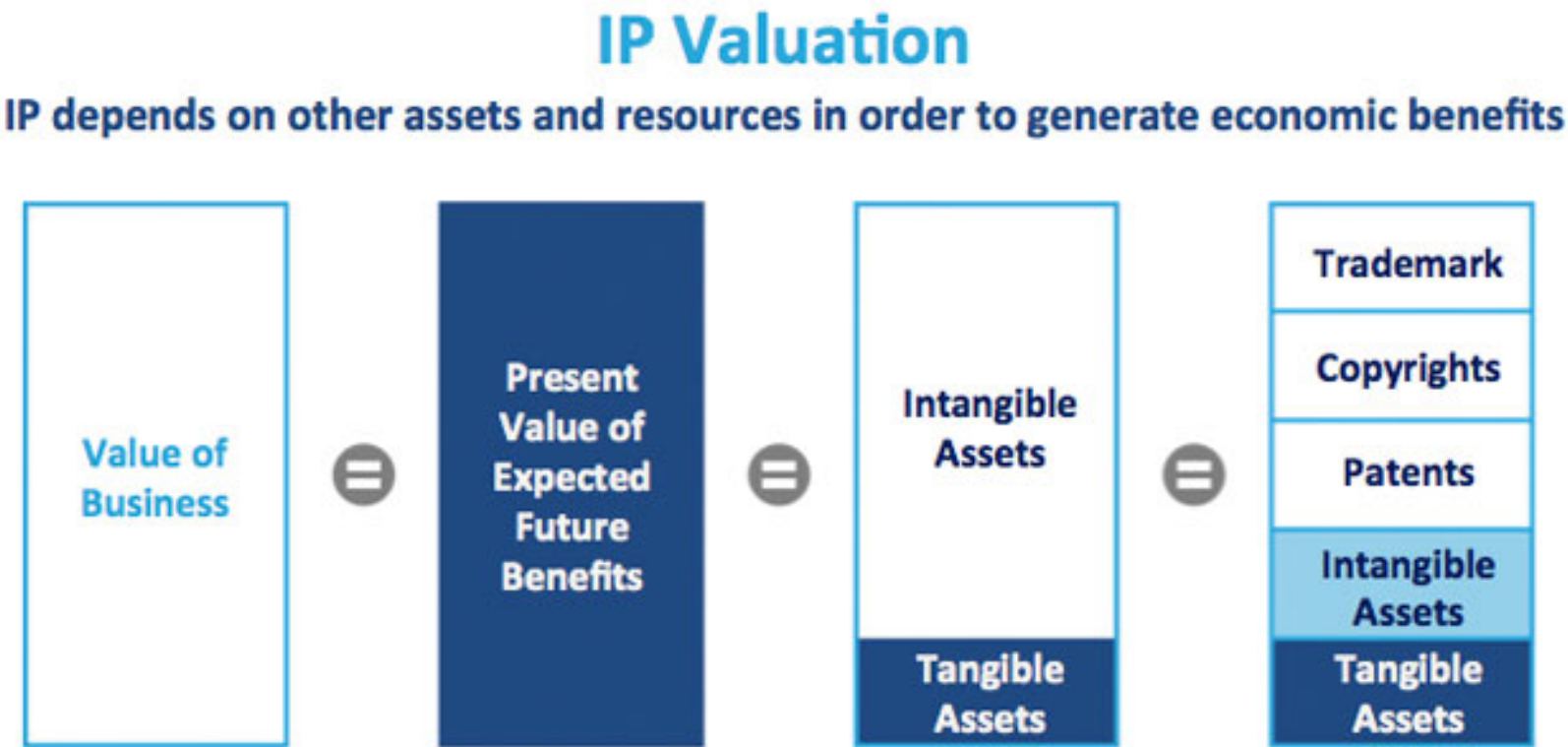


## Businesses Are Increasingly Valued By Intangible Assets

### COMPONENTS *of* S&P 500 MARKET VALUE



# Categories of Intangible Assets



# Patents Are Critical Assets In Bio/MedTech Company Valuations and Acquisitions



## Don't Neglect Data Security and Privacy

---

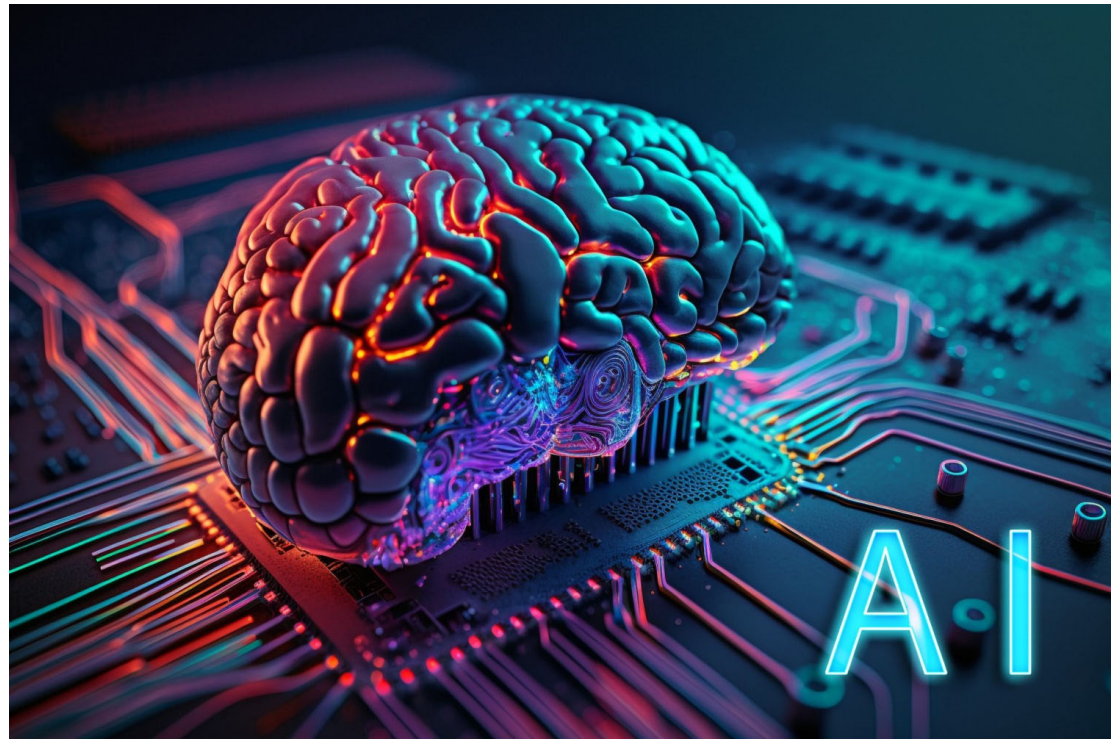


- 1 in 4 will experience a data breach.
- Cost of a breach can be about \$4M or more on average.
- Don't depend on privacy compliance alone—Be Proactive!

## Be Aware of How AI Can Help You and Harm You

---

- AI can Save Time and Resources in Development, but there are Risks
  - Know what AI tools are available.
  - Know what the terms of use are.
  - Understand the limits of the tools.
  - Understand the risks of infringing on the work of others.
  - Understand the risks related to ownership of developments.



# Protecting Innovation with Patents and other IP



## Protect Your Innovation with a Patent Fortress

- Control the Core
- Expand the Wall
- Prepare for Battle



## Control the Core – Evaluate Your Core Patent Position in an IP Audit

- Confirm ownership properly documented
- Foster communication between teams to confirm marketable features are protected by patent claims
- Incentives to encourage recording inventions



© 2024 Knobbe Martens



## Control the Core

---

- Secure rights with solid IP Agreements
  - Hire IP counsel for IP agreements
  - Execute strong NDA's before disclosing to others
  - Secure broad assignment agreements with all inventors
  - Be very careful with co-development agreements
    - Seek to own all IP
    - If not possible, define categories very carefully for ownership or use
    - Do not try to avoid the controversy through “co-ownership” of IP

## Control the Core

---

- Obtain meaningful patents
  - File early
  - Perform prior art searching and cite all prior art to examiner
  - Use expedited examination
  - Do not say conflicting things at Patent Office and FDA
  - Keep foreign options open in relevant markets

## Expand the Wall – File Continuing Patent Applications of Strategic Scope

- “IP Round-up”
- Foster communication about areas of future growth or expansion and direct patents to the space early on
- Encourage Provisional Patent Applications
- Protect Alternatives



© 2024 Knobbe Martens

## Expand the Wall

---

- Employ sophisticated patent claim strategies
  - Seek diverse coverage
    - devices and methods
    - Use varying claim scope and different specifications
  - Avoid claiming “too much”
    - Limit contextual structure
    - Be careful with reusable and disposable components
  - Use functional language
  - Always keep a continuation pending



## Prepare for Battle – Develop Strategic Offensive and Defensive Plans

- Conduct regular patent searching
- Foster communication about what is observed from competition in market
- Obtain opinions of counsel regarding third party patents of risk
- Craft claims to block competitor advancement



© 2024 Knobbe Martens

## Prepare for Battle

---

- Do freedom-to-operate searching and analysis
  - It is expensive but can dramatically enhance your company's valuation
  - Design-around where possible
  - Develop reliable non-infringement or invalidity arguments
  - Be careful about waiving attorney-client privilege in diligence discussions
  - Be wary of approaching IP owners to seek licenses

## Prepare for Battle

---

- Trade Secrets
  - Not a substitute for a patent
  - But can be very powerful in right circumstances
    - Must be kept secret; not easily reverse-engineered
    - Must be able to describe without disclosing secret
    - Strong contracts and diligent in keeping it secret

## Prepare for Battle

---

- Don't forget other IP issues
  - Trademarks
  - Copyrights
  - Domain names
  - Data privacy
  - AI considerations



# Respecting Privacy and Implementing Data Controls

## Trends in Med Device and Data Privacy

---

- Med Devices are sensing and collecting more data
- Med Devices are connected and transmitting more data
- Med Devices are provided access to more data
- Med Devices are learning and improving outcomes using data
- Data is becoming increasingly valuable
- Companies and Governments are respecting and protecting data

## Hypothetical Med Device Co makes standard pacemakers

---

- What kinds of data are involved?
  - Basic customer info?
    - Name, Address, Phone, Age, Birthdate?
    - Web IP address, shopping preferences?
  - Patient related data?
    - Health history? Mobile data? Heart rate?



- What are basic requirements for Data Privacy and Security?

## How should my Bio/Med Company respect and protect data?

---

- Companies should fully embrace data privacy and security
  - Take responsibility to respect the customer/patient re use of data
  - Take responsibility to secure the valuable customer/patient data
  - Comprehensive privacy and security plans will pay off long term
- Jurisdictions have new and developing laws
  - Understand the laws
  - Comply with the laws

## Examples of Comprehensive Data Rights Statutes

### CCPA v. GDPR



- Requires consent from the individual
- Wide definition of personal information including browser history, purchase behaviour, site/app interactions
- Allows for opt-out of collection/use
- Fines potentially in the millions of dollars
- Private right of action, class suits
- Extraterritorial effect on business



- Has a legitimate interest component
- Defines PII and sensitive information
- Default to opt-in for collection/use
- Fines potentially in the millions of dollars
- Public complaints to an enforcement body to address
- Extraterritorial effect on business


## Personal Rights under the GDPR

---

- Right to Access Personal Data
- Right to Rectification
- Right to Erasure
- Right to Restrict Data Processing
- Right to Be Notified
- Right to Data Portability
- Right to Object
- Right to Reject Automated Individual Decision Making

## Compliance Road Map

---

- 
- Create internal data privacy team, including point person, with relevant stakeholders
  - Obtain cyber insurance
  - Retain outside counsel
  - Consider retaining a company to assist with operations/IT
  - Conduct inventory of data collection and use
  - Prepare and update privacy policies and procedures
  - Prepare and update vendor agreements
  - Set up compliance mechanism for consumer access requests
  - Train personnel
  - Ensure PI is protected with adequate and reasonable security measures
  - Regular audits of privacy and security programs

## Privacy By Design – AI Considerations

---

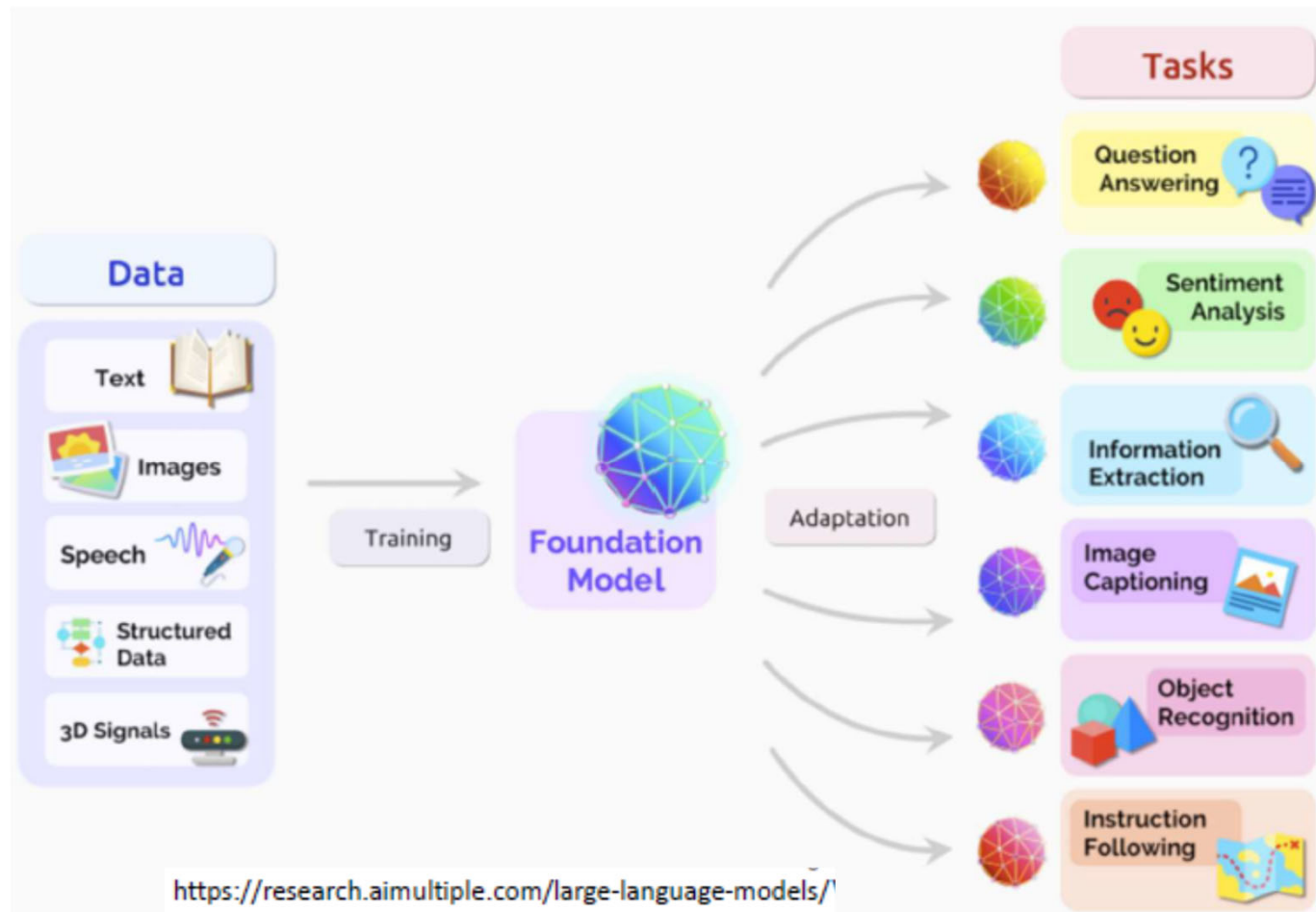
- Educate Engineers about Privacy
- Control Access to Data
- Minimum Data for Collection and Processing
- Strong De-Identification – Anonymous Data
- Beware of Quasi-Identifiers
- Ability to Handle Erasure and Rectification Access
- Know the process, explain the Logic – White Box vs. Black Box



# IP Considerations related to Generative AI

# AI – Large Language Models

- LLMs are deep learning neural networks, a subset of artificial intelligence and machine learning.
- LLMs are pre-trained so they learn basic language tasks and functions.
- Pretraining requires massive computational power and cutting-edge hardware.
- LLM capabilities are limited to training data. Models may learn or use false, biased, and/or IP protected information.



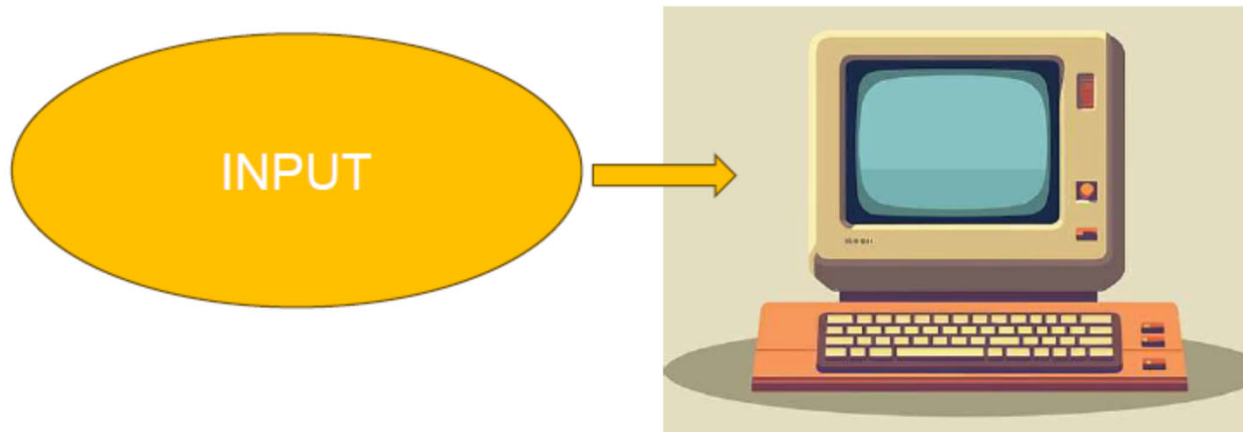
## Categorizing Generative AI Risk – Policy Considerations

---

- 1. Generative AI Input Risks
- 2. Generative AI Output Risks
- 3. Data Risks

# Categorizing Generative AI Risk – Policy Considerations

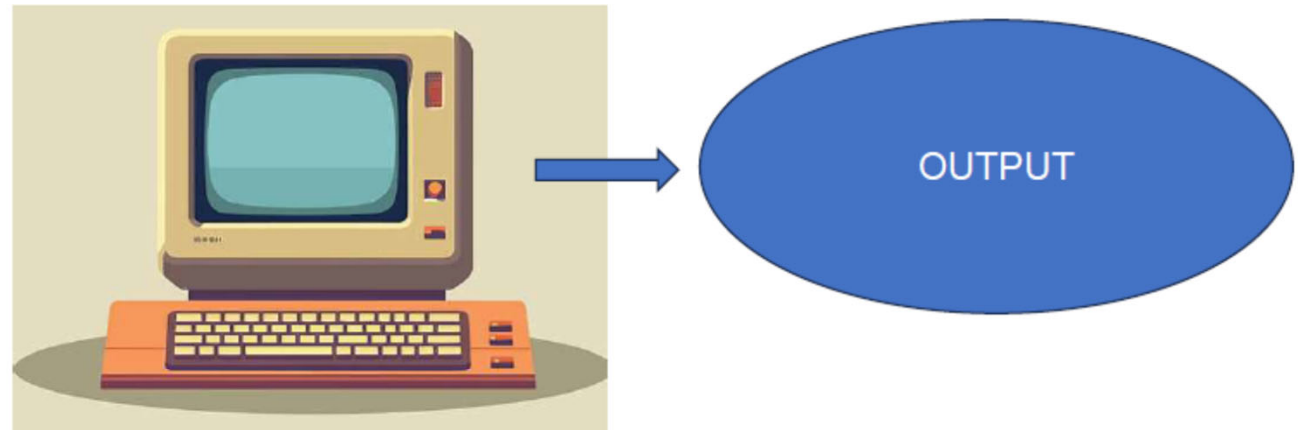
## 1 Generative AI Input Risks



- Many Generative AI tools (especially public versions) include terms of service that to varying degrees grant the AI / it's owner rights to use your inputs generally, for training the ML model, an/or generating future outputs.
- In many cases, your use of the Generative AI service and any input data submitted will not be considered confidential and may be publicly available.

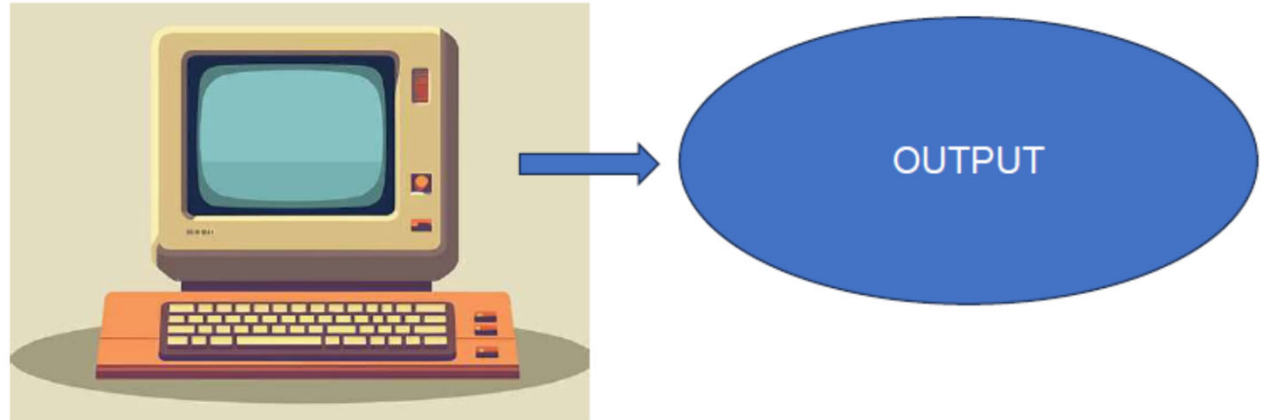
## Categorizing Generative AI Risk – Policy Considerations

- AI training data may have various licensing restrictions, or may be incorporated without necessary permissions - so use of outputs could lead to claims of copyright infringement, breach of licensing terms, etc.
- Outputs may also be duplicative of outputs provided to other users.
- Software code outputs may also be subject to different restrictive levels of Open-Source licensing obligations.



## Categorizing Generative AI Risk – Policy Considerations

- There are numerous examples of outputs from Generative AI that include incorrect or made-up information (e.g., hallucinations).
- AI may be trained on insufficient or incomplete data, or on data that includes errors, misconceptions, and biases.
- AI may be influenced by humans supervising its learning process and reinforcing or discouraging its decisions.



### 3 Data Risk

## FAQs on Use of AI – Complex Areas of Law Still In Development

---

- |   |   |
|---|---|
| 1. Is my INPUT confidential?  | <b>No – see Terms of Service</b>                    |
| 2. Is OpenAI's OUTPUT confidential? Unique?                             | <b>No – see Terms of Service</b>                    |
| 3. Do I <b>own</b> what OpenAI creates for me?                          | <b>Assume not – see Terms of Service</b>            |
| – Under what conditions?  | ● <b>Compliance w/ TOS; OpenAI has license</b>      |
| – With what possible consequences?                                      | ● <b>Risk of infringement, breach, inaccuracies</b> |
| 4. Can I create a <b>trade secret</b> with OpenAI?                      |   |
| 5. Can I get a <b>patent</b> on anything that OpenAI creates for me?    |   |
| 6. Can I get a <b>copyright</b> on anything that OpenAI creates for me? |   |
| – If so, what additional risks will I take on?                          |   |
| 7. Can I get a <b>trademark</b> on anything that OpenAI creates for me? |   |
| – If so, what additional risks will I take on?                          |   |

## Recommendations on AI

---

- Be aware of how AI is being used in your company, particularly with the development of technology, and investigate the risks.
- Consider ownership and protection of information
- Ensure that partners and contractors will not use AI without your knowledge.





Knobbe Martens

**Thank You!**

**Curtis Huffmire**

[Curtis.Huffmire@knobbe.com](mailto:Curtis.Huffmire@knobbe.com)