Association of Corporate Counsel
GREATER PHILADELPHIA

CONTRACTS FOR LICENSING ARTIFICIAL INTELLIGENCE SYSTEMS

What to Know

August 8, 2023

COZEN O'CONNOR

Presenters:

- Chris Dodson

  Member, Cozen O'Connor

  cdodson@cozen.com

- Andy Baer

  Chair, Technology, Privacy & Data Security Practice, Cozen O'Connor

  abaer@cozen.com

- Lauren Schmidt

  Associate General Counsel Global Legal Services

  QVC, Inc.

  lauren.schmidt@qvc.com

ACC Association of Corporate Counsel
GREATER PHILADELPHIA

Agenda

- What is Artificial Intelligence (“AI”) and How does it Work?
- Key Challenges Regarding the Use of AI
- Customer Pre-Contract Due Diligence on AI Vendors
- Representations and Warranties
- Infringement of Intellectual Property
- Intellectual Property Ownership and Use Rights
- Indemnification Obligations
- Limitation of Liability
- Privacy and Data Security Issues When Using AI
- Insurance
- Export Controls

What is AI and How Does it Work?

- AI generally refers to computer technology with the ability to simulate human intelligence to analyze data to reach conclusions about it, find patterns, and predict future behavior.
- AI is programmed to learn from data and adapt to perform certain tasks better over time.
- “Generative AI” means AI that can create new assets, like text, audio, images (including deep fakes), and software code. Examples include “large language models” like ChatGPT. Generative AI is trained through machine learning.
- “Machine learning” refers to creation of AI systems by “teaching” them, rather than just programming them. Machine learning systems can learn from past performance.

Key Challenges WITH AI

- Ownership of the training data and output data?
- Responsible for legal and regulatory compliance – vendor or user?
- Requiring AI vendors to engage in responsible and ethical AI practices
- Appropriate indemnification and limitation of liability
- U.S. and international privacy and data protection laws

Customer Pre-Contract Due Diligence on AI Vendor

- What are the assets or capitalization of the AI vendor?
- Does the AI system use personal data?
- Has the AI vendor been the subject of any complaints, regulatory inquiries, or litigation?
- How will the customer use the AI system?
- Will the AI system make decisions impacting individuals that are subject to specific laws?
- What is the scope of the AI systems' source data – was it captured "in-house" or scraped from "publicly available" sources?
- Will the data obtained by scraping only be used to train the algorithm, or may it also form part of the output of generative AI?

Representations and Warranties

A licensee should receive AI-specific representations and warranties:

- The AI system, including training data and output data, does not infringe third party IP rights. However, the responsibility for IP infringement is not a cut-and-dried issue (e.g., licensee may provide instructions, training data, etc.)
- The AI system, including training data and output data, does not violate any privacy or other personal or proprietary rights of any third party
- The AI system was developed and trained in accordance with the NIST AI Risk Management Framework or another equivalent artificial intelligence risk management framework
- The AI system, including training data and output data, does not violate any laws against discrimination or disparate impact

Notable AI-Specific Regulations, Laws, and Guidance

- FTC Guidance (April 2020)
- New York City's Automated Employment Decision Tool Law
- Illinois Artificial Intelligence Video Interview Act of 2020
- Equal Opportunity Employment Commission (EEOC) Guidance (May 2023)
- FTC Chair Khan and Officials from DOJ, CFPB and EEOC Release Joint Statement on AI (April 2023)
- Proposed European Commission's Regulatory Framework on AI (Originally Published April 2021)
- United Kingdom Government's White Paper on AI (March 2023)

Risk Management Frameworks

- National Institute for Standards and Technology (NIST) AI Risk Management Framework (January 2023) – Identifies six factors for mitigating risk and evaluating the trustworthiness of AI systems: (i) validity and reliability; (ii) safety; (iii) security and resilience; (iv) accountability and transparency; (v) explainability and interpretability; and (vi) privacy.
- Biden Administration Blueprint for AI Bill of Rights (October 2022) – Goals: (i) protect from unsafe or ineffective systems; (ii) protect from discrimination; (iii) protection of privacy; (iv) right to notice and explanation; (v) right to human alternatives, consideration, and fallback
- Worth Mentioning – Department of Energy AI Risk Management Playbook

Intellectual Property – AI Components

- Protected by copyright
  - AI system software (same as other software)
- Might be protected by copyright
  - Training data (depends on the data)
  - Is the use of training data a transformative fair use under copyright?
  - Exception: Japan – use of materials for AI training not copyright infringement
- Not protected by copyright
  - AI output data
  - Copyright Office: no human author, no copyright

Ownership and Use Rights - Training Data

- Ownership and Use of AI Training Data
  - AI training data: data set plus instructions about the data
  - AI agreement should cover which party will:
    - Provide and own the AI training data
    - Prepare and own the training instructions
    - Conduct the training
    - Revise the algorithms during the training process and own the resulting AI evolutions
- When possible, the agreement should identify the source of the data
- If training data includes personal information, address responsibility for data subject rights requests
- If licensee provides training data, the contract should designate it as confidential

Ownership and Use Rights – Output Data

- Output Data is what is produced by the AI system after training
- The parties should clearly establish who owns the AI output data
  - It is common for AI providers to assign ownership of AI output data to the licensee
  - AI providers may retain ownership of the AI output data and license the output data to the licensee for limited purposes
- If licensee will grant use rights in output data to third parties, ensure the contract with the AI provider allows it
- Licensees should be aware of privacy, data protection, and third-party restrictions that limit the use of the AI output data

Indemnification Obligations

- May be difficult to determine the cause of liability
  - Ex: if output data infringes a third party's IP rights, was it caused by the training data, the input of a user of the AI system, the AI system itself, or some combination of each?
- Licensee
  - Indemnification for
    - IP infringement
    - Breach of representations and warranties
    - Violation of laws
  - Should cover training data, the AI system itself, and the output (unless solely caused by a user's input)
- Licensor
  - Avoid indemnities for things that are outside of its control or are in the control of the licensee

Indemnification Obligations and Product Warranties

- Possible Compromises and Middle Grounds
  - Indemnification
    - “Super-Caps”
      - Seeking a super-cap for the most critical indemnities, such as such as IP infringement, confidentiality breaches, privacy and cybersecurity breaches, and customer data loss
      - Super-caps may be based on the greater of a specific dollar value or a multiplier based on contract fees paid or payable or some other formula (i.e., which may be tied to the amount of the vendor’s insurance).
    - Limiting the indemnification obligations to situations where a party breached its own obligations, as opposed to any or all incidents.
  - Product Warranties
    - Compliance with Laws
      - Compliance with a recognized safety or accountability framework (like NIST) or a limitation of remedies

Limitation of Liability

- As with any commercial agreement, when the parties are negotiating a liability cap in an agreement, they should look closely at the specific risks of the AI and apply individual limitations accordingly.
- In an AI license agreement, the risks associated with a system failure, security breach or inadvertent exposure of data can be disastrous.
  - If an AI system ingests a large volume of sensitive personal information, this increases the risk of highly sensitive personal information being exposed to downstream users. Licensees should consider excluding confidentiality and data privacy obligations from a limitation of liability provision.
- As liability for intellectual property infringement is uncertain and represents a substantial risk for licensees, licenses should consider excluding liability for intellectual property infringement from a limitation of liability.

Privacy and Data Security

- The AI agreement should require the parties to:
  - Comply with applicable data privacy laws
- The vendor should meet:
  - Licensee's security requirements;
  - The requirements of a recognized information security framework; or
  - Have a current third-party audit certification, such as a SOC II, Type II or ISO-27001
- The parties should consider the use of de-identified data
  - Many U.S. state privacy laws give users opt-out rights with respect to the automated processing of data for purposes of profiling.

Privacy and Data Security GDPR and U.S. State Privacy Laws

- **Consumer Opt-Out Rights for AI-Powered Decisions**
  - **California Privacy Rights Act: "**Automated decision-making technology"
  - **Virginia Consumer Data Protection Act, Colorado Privacy Act, Texas Data Privacy and Security Act, Indiana Consumer Data Protection Act, Oregon Consumer Privacy Act, Tennessee Information Protection Act, and Florida Digital Bill of Rights**: "Profiling in furtherance of decisions that produce legal or similarly significant effects" concerning the consumer
  - **Connecticut Data Privacy Act, Montana Consumer Data Protection Act, and Delaware Personal Data Privacy Act:** Opt-out right like the states listed above, but only for "solely automated decisions"
- **AI Transparency**
  - Colorado Privacy Act Rules require companies to include AI-specific transparency in their privacy policies about the "decisions" that are made by AI and subject to opt-out rights
- **General Data Protection Regulation**
  - Right to not be subject to a decision based solely on automated processing where that decision has a significant impact on them, subject to limited exceptions under Article 22(2)

Insurance

- As AI is an emerging area in technology, there are many possible ways AI systems can fail or cause damage.
- The insurance industry is evolving to address AI-related risks.
- Parties to an AI agreement should determine which form of coverage, if any, applies to any given situation.
- Insurance coverage also provides the other party some assurance that the insured party will be able to meet its indemnification and other obligations.

Export Controls

- Department of Commerce's Bureau of Industry and Security (BIS) imposes export controls on AI (January 2020)
- Biden administration announced a new export controls policy on AI and semiconductor technologies to China (October 2022)
- Department of Justice (DOJ) and the BIS announced a new enforcement initiative aimed at preventing and prosecuting evasion of US export controls on critical technologies such as semiconductors, artificial intelligence, additive manufacturing and advanced biosciences (February 2023)
  - Interagency Disruptive Technology Strike Force (Strike Force) brings together federal law enforcement resources "to target illicit actors, strengthen supply chains and protect critical technological assets from being acquired or used by nation-state adversaries"

Questions?

Andy Baer
Cozen O'Connor
Chair - Technology, Privacy & Data Security Practice Group
215.665.2185
abaer@cozen.com

Chris Dodson
Cozen O'Connor
Member - Technology, Privacy & Data Security Practice Group
215.665.2174
cdodson@cozen.com

Lauren Schmidt
QVC, Inc.
Associate General Counsel
Global Legal Services
Lauren.Schmidt@qvc.com

A reminder about the benefits of ACC membership…

- Free CLE, like the one you're attending right now
- Roundtables
- Networking meetings
- Special events (Spring Fling, Fall Gala, races, etc.)
- Access to ACC resources, including:
  - ACC Newsstand (customizable updates on more than 40 practice area)
  - ACC Docket Magazine
  - InfoPAKs
  - QuickCounsel Guides

- **For more information or to refer a new member, see your hosts today or contact Chapter Administrator, Chris Stewart, at ChrisStewart@ACCglobal.com.**

ACC Association of Corporate Counsel
GREATER PHILADELPHIA