Artificial Intelligence:
Key Uses and Risks, and the Legal Landscape

CLARIO.

Weil

Agenda

I. Introduction

II. Legal Landscape

III. AI Risk Management

IV. Governance

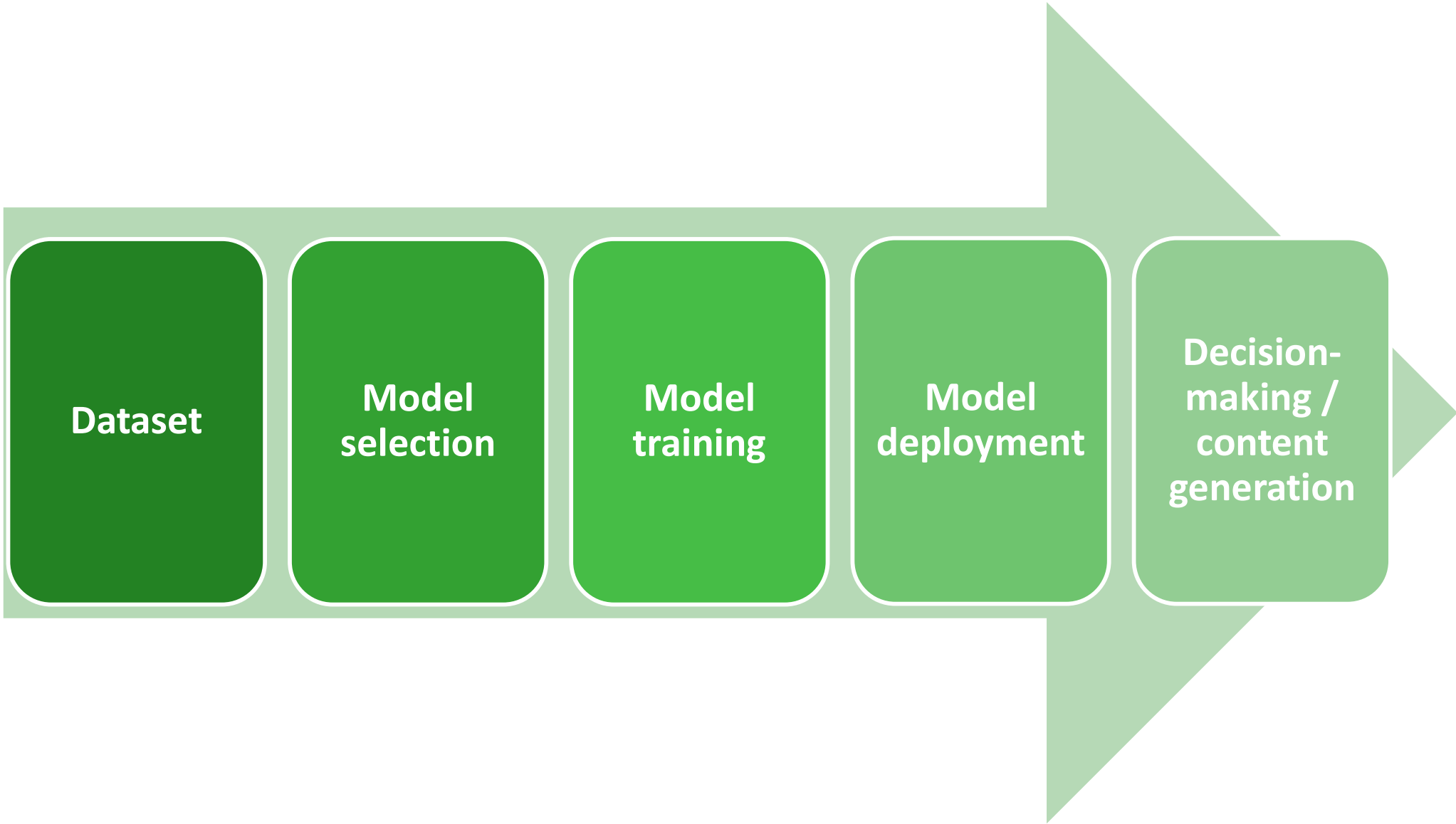
I. Introduction

What are we talking about?

Weil

Artificial intelligence (AI)	…makes it possible for machines to learn from experience, adjust to new inputs and perform human-like tasks.
Generative AI	…is AI capable of generating text, images, or other media, using generative models (a type of machine learning model that aims to learn the underlying patterns or distributions of data to generate new, similar data).
Artificial general intelligence (AGI)	…is a (theoretical?) form of AI that can understand, learn and apply knowledge across a wide range of tasks and domains.

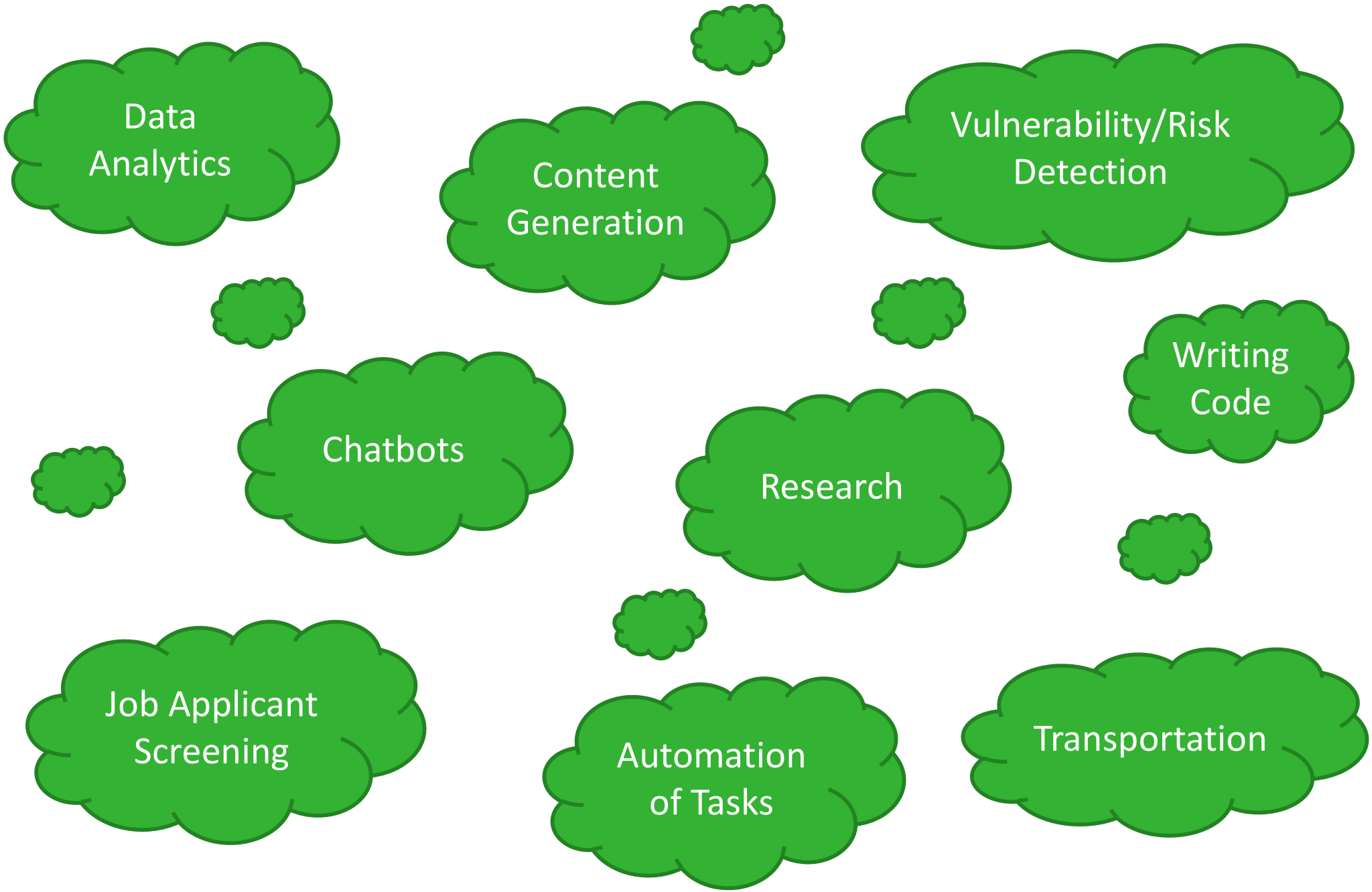
What Does It Mean To Train AI?



Consumer AI vs. Enterprise AI

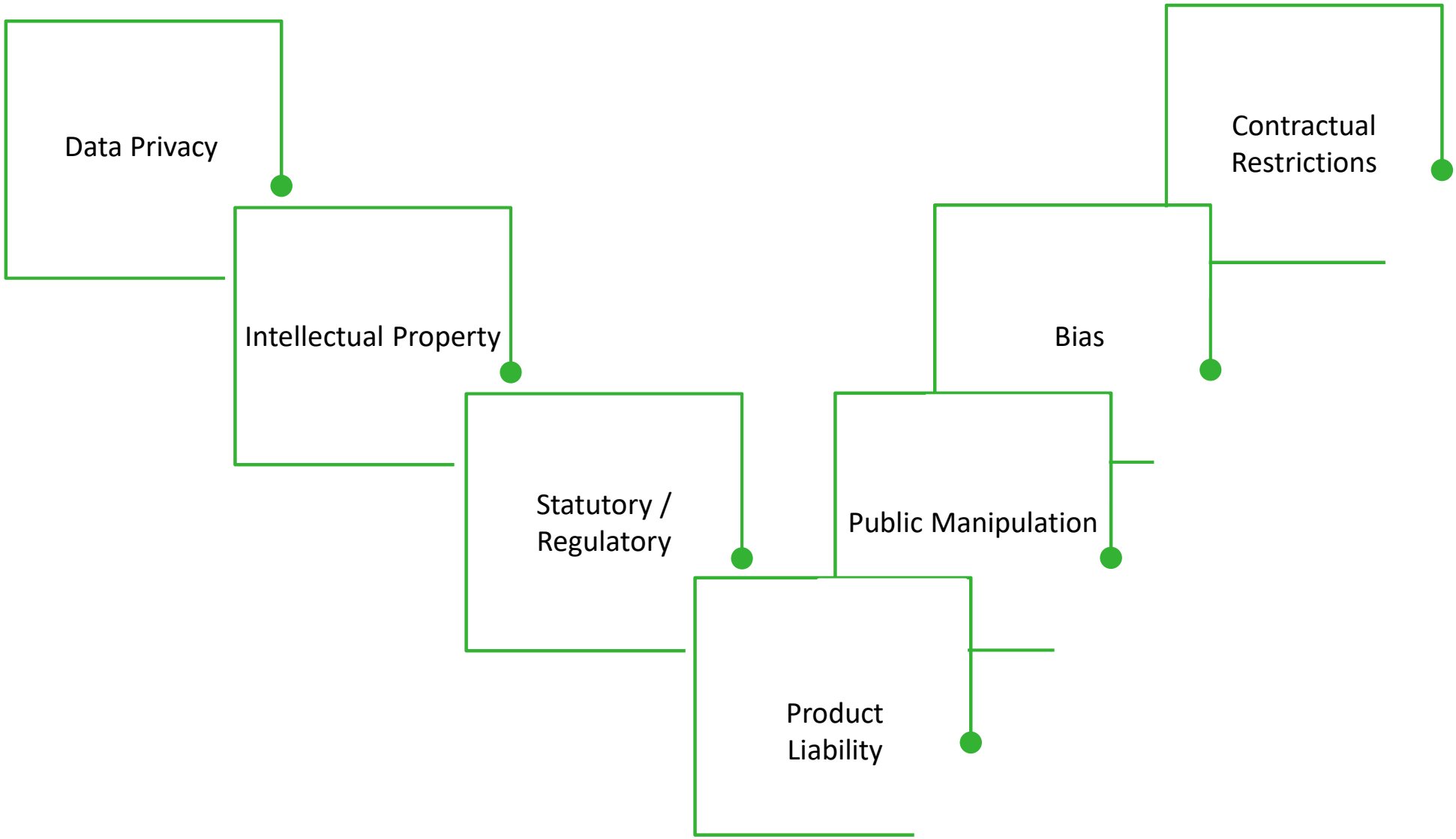
Consumer AI	Enterprise AI
• Available for use by the general public	• Designed for business functions
• Models have been trained on large, general datasets	• Models may be fine-tuned on topic-specific datasets
• Most providers reserve rights to use input data for future training	• Commercial terms may restrict providers from using inputs

How is AI being used right now?



II. Legal Landscape

Key Areas of Legal Risk



U.S. State AI Legislation

- **Insurance**:
  - Colorado SB 21-169 took effect on Jan. 1, 2023, seeking to prevent discriminatory insurance outcomes from predictive modeling to underwrite policies and process claims
- **Employment:**
  - Illinois, Maryland, New York City have enacted laws regulating the use of "automated employment decision tools" or "predictive data analytics" used by employers to make hiring, termination, promotion or compensation decision
- **Elections:**
  - 5+ states have enacted laws aimed at restricting the use of manipulated media content in connection with election cycles, including requiring disclosures on manipulated content, banning deepfake content, etc.
- **Privacy:**
  - Omnibus state privacy laws include restrictions and rules concerning profiling and automated decision-making

Intellectual Property: Copyright & Patent Issues

- **U.S. Copyright Office:** copyright protection extends only to ***human creativity***.
  - *Assistance vs. Generation.* Is the work one of human authorship with AI assistance or are the traditional elements of authorship (*e.g.,* creative expression) conceived and executed by the AI?
  - *Modified Generative AI Works?* An artist may modify material originally generated by AI to such a degree that modifications meet the standard for copyright protection.

- **USPTO:** patentability is possible only if ***significant human contribution*** is present for every claim in a patent.
  - *AI Ownership & Management?* Ownership or oversight of AI is insufficient.
  - *Reduction Absent Invention?* Reduction to practice of an invention *is not* itself *a significant contribution*.
  - *Key Underlying Developments.* Development of an essential aspect of an invention may be a significant contribution even if the inventor was not a participant for each step of a claimed invention.

Intellectual Property: Infringement and Other IP Risks LM0

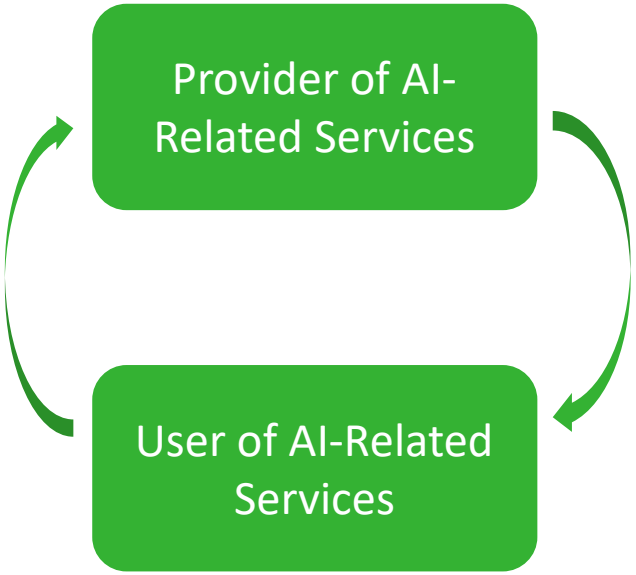
- ***Direct or Secondary Copyright Infringement.*** Various copyright infringement claims, such as those based on AI outputting content whose use, reproduction, etc. infringes the copyright in training materials (see for example *New York Times vs. OpenAI & Microsoft*).
- ***Direct, Indirect, Induced or Contributory Patent Infringement.*** Development of an AI system could result in an infringement claim, such as if a patented algorithm or training process is used without a license. Further, AI-generated solutions may inadvertently infringe a similar already-patented solution (*e.g., synthetic biologists engage AI to optimize a molecule, but the resulting molecule is covered by another company's patent*).
- ***Removal of Copyright Management Information.*** Digital Millennium Copyright Act ("DMCA") prohibits the removal of any "copyright management information" (identifiers of authorship).
- ***Trademark Infringement or Dilution.*** AI-generated materials can include designations that are attributable to a business' trademarks. Consider whether AI outputs create a "likelihood of confusion" among consumers.
- ***Misappropriation of Name, Likeness, Voice or other Personal Characteristics.*** AI-generated material can imitate (intentionally or otherwise) an individual's personal characteristics thus resulting in a misappropriation claim (*e.g.*, business created fake product endorsements using AI-generated voices of prominent celebrities).
- ***"Fruit of the Poisonous Tree."*** As applied to AI, the doctrine would consider whether an entire AI system is infringing solely because during development certain IP infringement activity occurred.

Slide 12

LM0 Potentially mention considerations re whether to patent an AI algorithm ~ risks to disclosing it v/ benefits of patent protection

Lauren Misztal, 2024-09-10T19:08:40.025

Privacy Considerations



Is personal data in the inputs, training data, outputs?

LM0

Which party is responsible for decision making?

Are data protection principles satisfied?

Transparency | Minimization | Legal Basis

Risk Assessment | Data Subject Rights

How do data subjects exercise their privacy rights?

Is there automated decision-making (profiling)?

What contractual provisions may be necessary?

Slide 13

LM0 Potentially comment re anonymization

Lauren Misztal, 2024-09-10T19:17:20.997

FTC & Algorithmic Disgorgement

Weil

RITE AID — Dec. 2023

- Allegedly deployed facial recognition technology for security/surveillance purposes without:
  - Sufficient notice to customers;
  - Considering the accuracy of vendor facial recognition technology before deploying it;
  - Implementing appropriate safeguards to prevent bias, false positives and other consumer harm;
- Proposed order:
  - Banned from using facial recognition technology for surveillance purposes for five years;
  - Implement safeguards to prevent consumer harm when deploying automated systems that use biometric data;
  - *Delete (and direct vendors to delete) all images collected in connection with facial recognition system and any algorithms or other products developed using that data*

Cambridge Analytica — Dec. 2019

everalbum — May 2021

WeightWatchers — March 2022

ring — May 2023

alexa — July 2023

Bias in AI

University of Chicago News

AI is biased against speakers of African American English, study finds

Large language models attributed negative attributes, less prestigious jobs and more convictions to speakers.

2 days ago

WH Executive Order 13985 directs federal agencies to ensure that their own use of artificial intelligence and automated systems also advances equity.

nea National Education Association | NEA

Does AI Have a Bias Problem?

As AI technology increases in classrooms, so do the concerns about perpetuating bias in education.

Feb 22, 2024

Colorado SB24-205 will govern how AI is used in evaluating people in connection with school applications, hiring, loans, access to health care, insurance.

Modern Healthcare

Senate leaders seek tougher AI bias protections from White House

Senate Majority Leader Chuck Schumer wants the White House to tighten civil rights safeguards against faulty algorithms for all recipients...

3 days ago

The Supreme Court & Legal Risks Looking Forward

Weil

- The Supreme Court has not yet squarely addressed AI-related issues, but several recent cases suggest that the Justices are concerned about AI and how it fits into existing legal frameworks.
  - In concurrences and dissents in *Moody v. NetChoice*, Justices Barrett and Alito expressed skepticism about First Amendment protections when a platform uses AI tools to curate or filter third-party content.
  - At oral argument in *Gonzalez v. Google*, Justice Gorsuch expressed skepticism that AI-generated content could be protected by Section 230 of the Communications Decency Act.
  - On the copyright side, the Supreme Court in *Andy Warhol Foundation v. Goldsmith* called for very close inquiry into how exactly a copied image is used, to determine whether that is a "fair use". That decision suggests that the Court would use a similarly nuanced approach to fair use issues arising from AI models.
- These issues are in flux.
- Counsel should recognize the uncertainty regarding the application of existing legal frameworks to AI tools and AI-generated content.

EU/UK Privacy Regulators & AI-Related Actions

Weil

CNIL.	CNIL publishes recommendations on the development of artificial intelligence systems to balance innovation and individual rights	Jun. 2024
ChatGPT	After temporary order in March 2023, Italy's Garante again notified OpenAI that its data processing activities violate the GDPR; OpenAI to submit response by Feb. 28	Jan. 2024
ChatGPT	EDPB announces "dedicated task force to foster cooperation and to exchange information on possible enforcement actions conducted by data protection authorities."	Apr. 2023
CNIL.	CNIL releases "how-to" on the creation of data sets to train AI models, aimed at supporting innovation while ensuring data protection compliance	Oct. 2023
ChatGPT	Poland announces investigation into OpenAI's data processing activities in response to complaint filed by privacy researcher alleging GDPR violations (incl. rights requests)	Sept. 2023

EU AI Act: The Basics

- **Status**: Enacted on August 1, 2024
  - Fully enforceable in 24 months; with notable exceptions:
    - 6 months for provisions re: prohibited AI
    - 12 months for provisions re: general-purpose AI
    - 36 months for provisions re: high-risk AI systems

- **Fines:** Higher of €7.5 – 35 million or 1 – 7% worldwide annual turnover (depending upon the breach)
- **Regulators:** National competent authorities to be designated (within 12 months of enactment). European AI Board established. AI Office.

EU AI Act: Who and what does it apply to?

- **AI systems**: "a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments"
- **General Purpose AI (GPAI) models:** AI models that are capable of competently performing a wide range of tasks and can be integrated into a variety of downstream systems or applications
- **Key actors in the AI value chain**: providers, importers, distributors, deployers (users)
- **Scope**:LM0
  - Providers placing AI systems in the EU (irrespective of where they are established)
  - Deployers using AI systems in the EU
  - Providers and deployers of AI systems located outside the EU where the output of such systems is used in the EU

Slide 19

LM0 There is a carve out vis-a-vis AI systems used for the sole purpose of scientific research and development.
Lauren Misztal, 2024-09-10T19:54:39.517

EU AI Act: A Risk-Based Approach for AI Systems

Weil

Risk Classification	Examples	Obligations	
		Providers	*Deployers*
Unacceptable Risk *Significant risk of harm from manipulative, exploitative and social control practices*	▪ Behavioral manipulation ▪ Social scoring ▪ Emotion recognition systems used in the workplace and educational institutions	Prohibited entirely as of 6 months after enactment.	
High Risk *Significant risk of harm to the health, safety, or fundamental rights of natural persons*	▪ Remote biometric identification systems ▪ Biometric emotion recognition systems ▪ Creditworthiness and credit score ▪ Life and health insurance pricing ▪ Recruitment selection ▪ Education and vocational training ▪ Safety components of certain products where already regulated under EU law *See full list of areas and systems included in Annex III at Slides 34 to 36*	▪ Risk assessments ▪ Quality of datasets ▪ Logging/traceability ▪ Transparency ▪ Human oversight ▪ Security & accuracy ▪ Quality management system ▪ Registration ▪ Conformity obligations ▪ AI literacy	▪ Comply with provider instructions ▪ Human oversight ▪ Quality input data ▪ Retention of logs ▪ Transparency ▪ Specific-use related obligations ▪ AI literacy
Limited Risk *AI systems intended to interact with individuals or generate content that may pose risks of impersonation or deception*	▪ Chatbots ▪ Virtual assistants (e.g. Siri) ▪ AI systems generating deepfakes	▪ Transparency, *if not obviously AI* ▪ Technical measures, if produces synthetic images, audio, video or text ▪ AI literacy	▪ Transparency, *if generates or manipulates images, video or audio* ▪ AI literacy
All other AI systems (Minimal risk)	▪ Autocorrect ▪ Photo recognition features	▪ AI literacy	

EU AI Act: General-Purpose AI Models (GPAIs)

Weil

GPAI Models	
What is it?	▪ An AI model that displays significant generality and is capable of competently performing a wide range of distinctive tasks and can be integrated into a variety of downstream systems or applications ▪ Two types: (1) "GPAI model" and (2) "GPAI model with systemic risk". ▪ "Systemic risk" – broadly, such a powerful model that it could have a negative effect on public health, safety, security, fundamental rights, or the society as a whole. ▪ GPAI model v GPAI system: a GPAI AI system is an AI system based on a GPAI model, that has the capability to serve a variety of purposes, both for direct use as well as for integration in other AI systems
Obligations	▪ **Technical documentation**, including training and testing process. ▪ **Documentation for providers**, to help providers understand the AI system to help understand the AI model ▪ **Copyright policy** ▪ **Publicly-available summary about content used to train the model** ▪ **GPAI models with systemic risks**: additional obligations for e.g. model evaluations, reporting and cybersecurity obligations. ▪ **Authorised representative** (if established outside EU).
Examples	GPT-4 (OpenAI), DALL-E (OpenAI), Gato (DeepMind), PaLM 2 (Google)

Ex-U.S. & EU/UK

Weil

Statement of Intent → **Draft Legislation** → **Legislation**

- **Australia:** government announces intention to regulate high-risk AI
- **India**: government considering adding AI-specific rules to existing or new laws

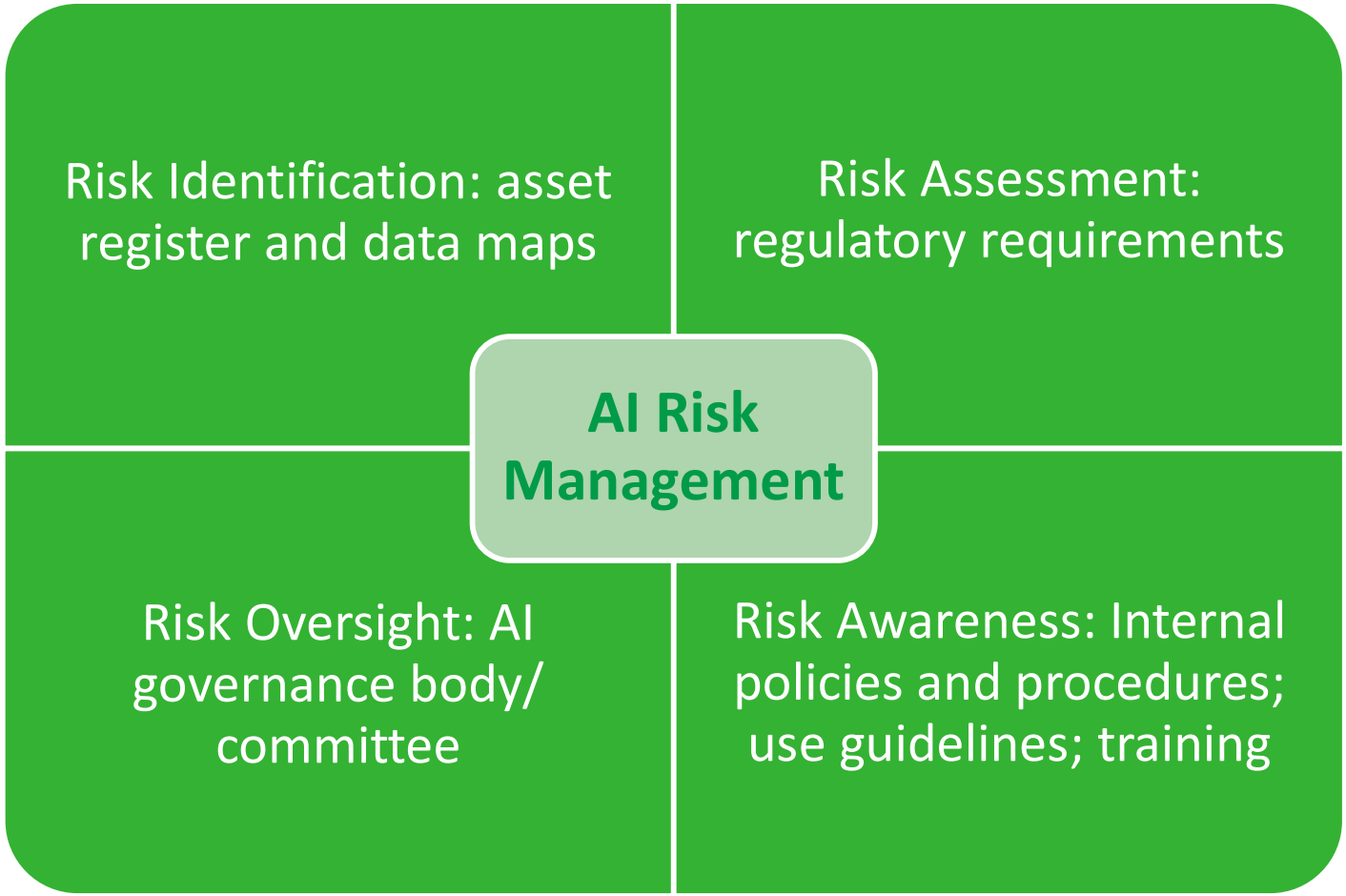
Draft AI bills in **Mexico, Chile, Peru, Brazil, Philippines**

China:
- Specific existing legislation regulates certain AI applications (rec. algorithms, deep synthesis technology, generative AI).
- Broad legislation being considered.

AI codes of conduct, ethical principles and guidelines in numerous other jurisdictions

III. AI Risk Management & Governance

AI Risk Management



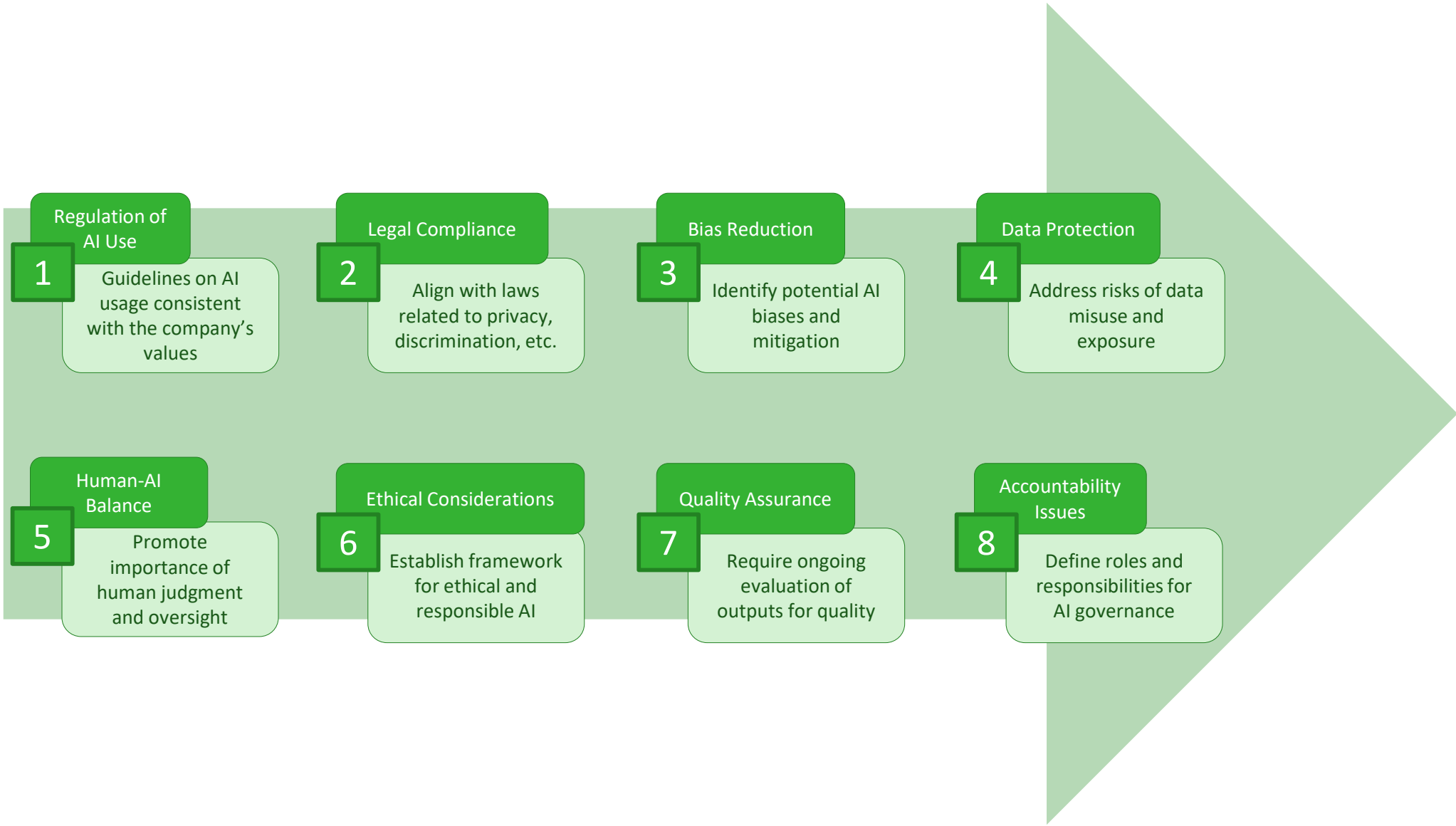
AI Governance Body

Objectives | Mission Statement

To establish a robust framework for the responsible development and deployment of artificial intelligence, prioritizing transparency, fairness, accountability, and human oversight, ensuring that AI technologies are used ethically and contribute positively to society while mitigating potential risks.

Chief AI Officer, Chair				
Legal & Regulatory, Member	Technology / R&D, Member	Commercial / Product, Member	Data Privacy, Member	IT Security, Member
Quarterly Meetings with Designated Secretary				

AI Governance Policies / Guidelines



AI Governance Framework

Weil

Clario's commitment to the responsible use of AI

Minimizing bias

To reduce the potential for biased or unjust results, we use the most diverse data available to train the algorithms incorporated into our products and services

Ensuring Accountability

We offer explanations of the intended purpose of the AI, the data inputs used for training and validation of the algorithms, and what/how decisions are made by AI-enabled tools

Regulatory Landscape

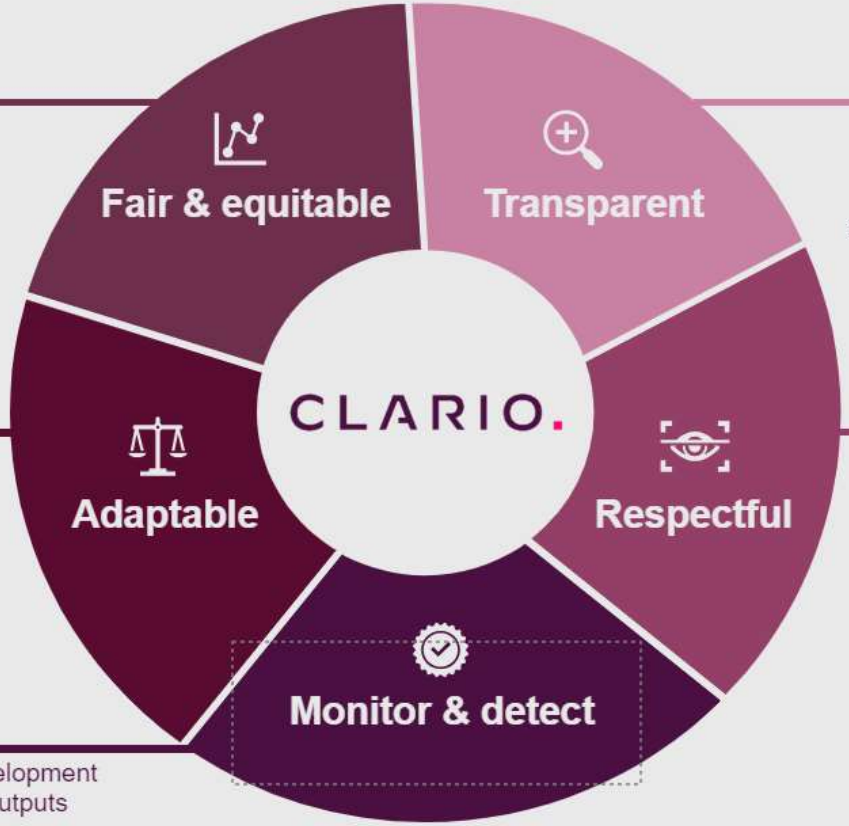
To comply with applicable regulations as they come into force, we are committed to continuously monitoring the rapidly evolving regulation of AI

Privacy Rights

Our compliance with global data privacy laws and regulations is a priority. Using fully anonymized data to train AI models, the data is not traceable to any specific clinical trial, study sponsor, or study participant

Mitigating Risks

We integrate human oversight into development and use of our AI solutions to monitor outputs for accuracy and reliability



AI in Contracts

Weil

Assignment / Licensing	• Will the data / algorithm / software be assigned or licensed? • Exclude implied licenses
Improvement / Development Ownership	• Who owns the data and algorithms (i) collected or developed, or (ii) derived or resulting from use of provided data?
Reps & Warranties	• IP; privacy; compliance with specs, contract obligations, and law; data security; absence of defects and viruses.
Closing Covenants / Conditions	• Removal or segregation of non-compliant data sets • Shut down of non-compliant products / services
Indemnification & Limits of Liability	• Tailor to address gaps in the law, in particular product liability law
Termination	• Will non-compliance with reps or other obligations lead to termination? • What is the right cure period? • Do parties cease performance during non-compliance?
Insurance	• Consider both third party claims and first party coverage
Dispute Resolution	• ADR or litigation?
Confidentiality	• Protect non-public proprietary information from disclosure
Applicable Law	• Watch for evolving state laws, federal/state regulation, agency guidance, ex-U.S laws and regulations (Australia, Brazil, China, Chile, EU, India, Mexico, UK)

AI in Contracts: Vendor Agreements

- Clear articulation of purpose(s) and use case(s) for the tool
- Whether any model fine-tuning is required and, if so, clear identification of training datasets
- Categories and sources of input data
- Vendor's rights to use the contracting party's data
- Data protection and confidentiality terms
- Indemnification provisions and other terms governing liability

AI in Contracts: NDAs

Weil

	Data Provider	Data Recipient
Definition of confidential information	Seek a broad definition so as much shared data as possible is within the scope of protections	Target/define categories of data to allow for flexibility with as much data as possible
Usage Rights	Limit recipient's ability to use confidential information in connection with AI systems/tools	Retain ability to use AI tools in analysis and diligence processes
AI Training	Prohibit use of data for model training or other uses out of scope of the activities contemplated under the NDA	It is market to commit to refraining from using confidential information for purposes out of scope of the NDA activities

Key Takeaways

Weil

Fairness	Transparency	Legal Rights	Accountability	Human Oversight	Security

- Regulators are keenly focused on transparency – disclosure and reporting – and the consequences are becoming more consequential
- Understand your use cases – how your business is using AI tools, and why, and where the risks could be.
- Make sure your statements about AI, data handling, security and other related issues match your practices (advertisements too)
- Oversight, as well as lines of communication and reporting are critical – teams must know how and when to escalate
- Know what your contracts (with customers, partners, and vendors) require you to do in connection with artificial intelligence technologies
- Developing laws and regulatory schemes create ongoing implementation challenges and require discussions about risk
- Revisit use cases, risks and guardrails regularly as the technology (and the legal landscape) changes

Discussion and Questions