FROM ALGORITHMS TO INSIGHTS: NAVIGATING AI PRODUCT COUNSELING

Elliot Golding and Shannon Ralich

November 9, 2023

McDermott Will & Emery

SPEAKERS

ELLIOT GOLDING

Partner
McDermott Will & Emery

egolding@mwe.com

SHANNON RALICH

VP, Interim Chief Privacy Officer, Associate General Counsel, Privacy
Zendesk

AGENDA

1. What is artificial intelligence?

2. How is artificial intelligence regulated?

3. How to evaluate AI use cases, reduce risks, and “get to yes”

WHAT IS ARTIFICIAL INTELLIGENCE?

DEFINING “ARTIFICIAL INTELLIGENCE”

- What is the hallmark?
  - Automated decision-making?
  - Responding to open-ended inputs?
  - Self-training/“learning”?
  - Generating “creative” content?
  - Ability to imitate humans?

WHAT IS ARTIFICIAL INTELLIGENCE?

- AI = using computers to complete tasks that usually require human intelligence.
- AI “learns” by looking at training data, user inputs and outcomes.
- Examples of AI:
  - Voice assistants and spoken language processing
  - Free text, speech and facial recognition
  - Financial data/fraud analysis
  - Customer service chatbots
  - Language to text/image generation
  - Combined environment and human systems
- **NOT** robotic process automation

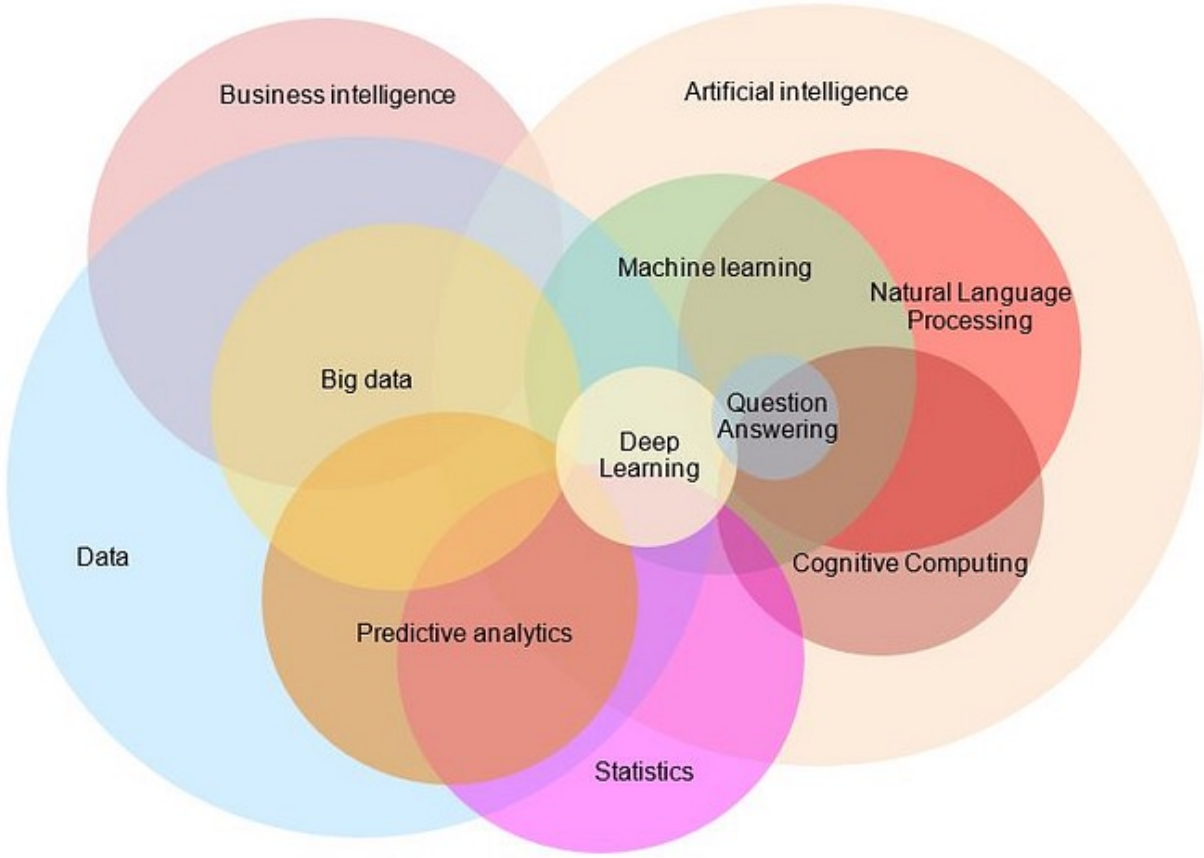


Image Source: https://medium.datadriveninvestor.com/how-my-computer-copies-a-baby-machine-learning-types-5ffc8add6b31

LARGE LANGUAGE MODELS (LLMS)

Model

Input-output algorithms that learn—i.e., adjust their internal variables by trial and error using data

Language

Takes input as a window of text, generates new text by predicting the next word, repeatedly

Large

Many variables, and usually trained on a huge dataset of examples

HOW IS ARTIFICIAL INTELLIGENCE BEING REGULATED?

US LANDSCAPE REGULATING AI

- Legislation is slow to develop:
  - Pacing problem – technology moving faster than legislation
  - But legislation and regulation is on the way
  - Requirements will likely include transparency about use of AI
- FTC, DOJ, CFPB, EEOC
- US state privacy
  - Right to opt-out of automated decision-making (e.g., CA, VA)
  - Access requests for underlying logic and likely outcomes
- Pending US state bills regulating AI
- NIST, ISO

DRAFT CCPA REGULATIONS

- Broad definitions of “artificial intelligence” and “automated decision-making technology”:
  - “Artificial intelligence”: engineered/machine-based system that can generate outputs such as predictions, recommendations or decisions
  - “Automated decision-making technology”: system, software, or process that processes PI and uses computation to make a decision
- Requirements for risk assessments, transparency

EU ARTIFICIAL INTELLIGENCE ACT: OVERVIEW

Status

Pending

- Vote in the EU Parliament – June 14, 2023, followed by trialogues with the Council and the Commission
- September 28, 2022, the Commission published proposed amendments to Product Liability Directive and new AI Liability Directive which will sit alongside the AIA.

Key Aims

- Ensure that AI systems are safe and respect EU fundamental values
- Create legal certainty to facilitate investment and innovation in AI
- Establishes tier system

Key rights & obligations

- Prior risk assessments
- Respect for fundamental rights
- Transparency towards users
- Post-market monitoring and reporting
- Human oversight
- Restrictions on certain use cases

Sanctions

- National authority
- European Artificial Intelligence Board
- Fines up to 30 million EUR or up to 6% of worldwide annual turnover (40 million EUR / 7%) for most serious non-compliance

HOW TO EVALUATE AI USE CASES, REDUCE RISKS, AND “GET TO YES”

WHAT'S THE USE CASE?

Building or Buying AI Solution	Data Generation	Outcomes
The AI tool/software is the product/service	The "input data" is the product/service	AI used as part of service to provide "output data"

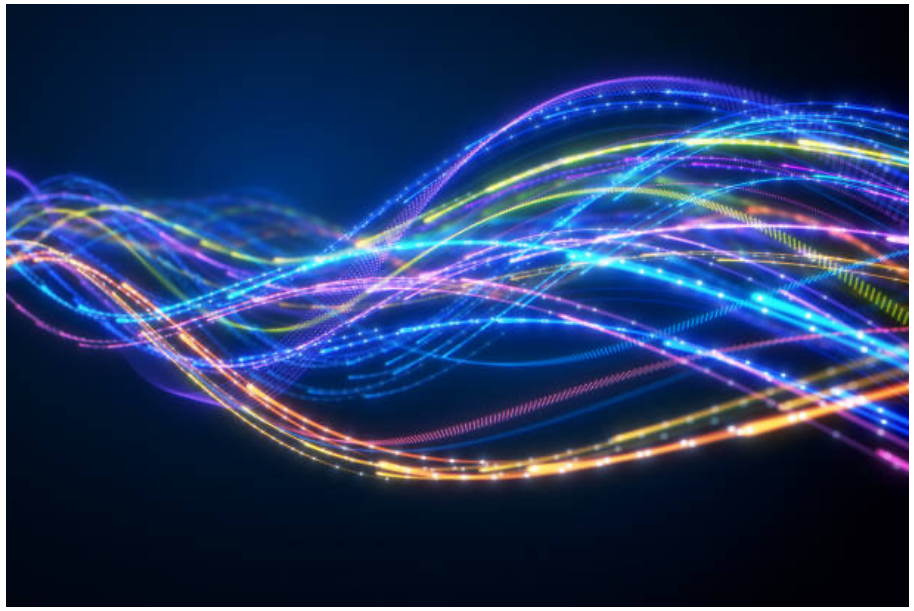
KEY CONSIDERATIONS TO GUIDE DECISION-MAKING

How important are each of the following (relatively)

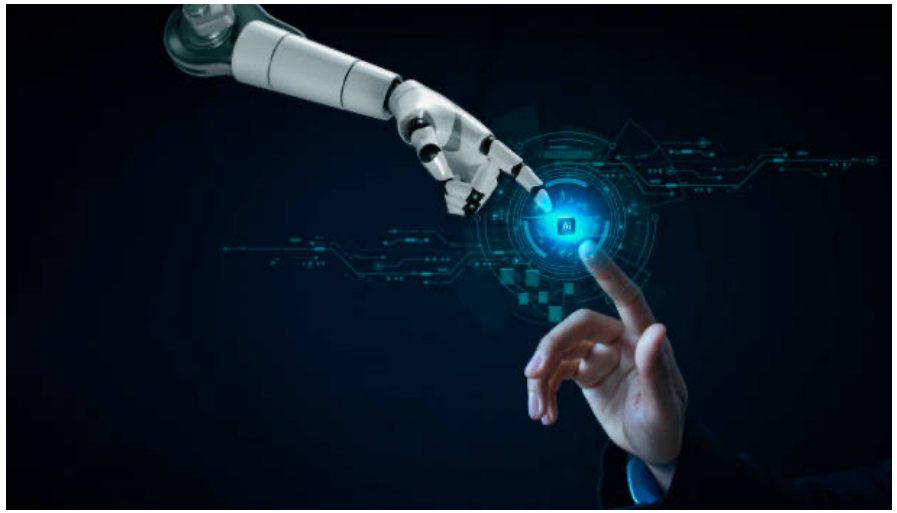
- Compliance cost & timing
- Data/technology flexibility
- Commercial feasibility
- Brand/image, trust, & accountability
- Internal Resource Issues
- Other

FRAMEWORK FOR EVALUATING

1. Where data comes from/is processed
   - Sources and which laws apply
2. Role/responsibilities for data
   - Controller vs. processor
3. Data used
   - Identifiable vs. de-identified; sensitive data
4. Uses of data
   - “Optimization” vs. automated decision-making
5. IP rights
   - Preserving rights in input, output data
   - Not violating others’ IP rights



FRAMEWORK FOR EVALUATING (CONT.)



6. Implementation
   - Cross-platform vs. for a single customer
   - Consent flows
   - Integrating with other providers (e.g., BYOAI)
   - Data retention and maintaining training data sets
7. "Soft" risks
   - Optics, reputation, ethical harms, industry expectations
8. How to communicate risks to audience
   - E.g., internal engineers, executive/sales, marketing/comms, executives, customers (business), end users/consumers

“GETTING TO YES” STEP 1: KEY DATA QUESTIONS

1. Do you really need identifiable/sensitive data?
   - Get to “yes” by using de-identified data.
   - Get to “yes” by avoiding SPI (otherwise consent often needed).
   - Get to “yes” by avoiding “higher risk” jurisdictions
2. Do you have rights to the data?
   - Get to “yes” by using existing data for purposes disclosed in notice
   - Get to “yes” by positioning as controller vs. processor
   - Get to “yes” by obtaining licenses/reps from third parties

“GETTING TO YES” STEP 2: USE CASE QUESTIONS

1. Is it a new use case?
   - Get to “yes” by fitting into existing disclosures/contract rules; OR
   - Get to “yes” through “just in time” notice/consent if needed
2. Is the use case highly regulated?
   - Get to yes by avoiding “highly regulated” uses
     - Is it ***really*** AI (vs. analytics)?
     - Is it ***really*** selling/sharing?
     - Is it ***really*** making “automated decision-making” (vs. providing options)?

“GETTING TO YES” STEP 3: COMMERCIALIZATION ISSUES

1. Can the risks be outsourced?
   - E.g., through contracts or consent forms
2. Can risk be managed by tweaks to marketing/commercialization strategy
   - E.g., tone down product feature description
   - E.g., structure as B2B vs. direct to consumer

TO SUM UP: RISK MITIGATIONS

- Governance frameworks
  - Internal procedures for evaluating new uses of data, development, and deployment of AI tools
- Acceptable use policies
  - Policies for use of third-party generative artificial intelligence tools (customized based on tool, role, etc.)
- Contracting procedures
  - Privacy, confidentiality, and IP considerations

QUESTIONS?