What Happens When Your Speed of AI Innovation Exceeds Your Ability to See the Regulatory Challenges Ahead?

May 17, 2022

Robert E. Cattanach, Partner

Dorsey & Whitney, LLP

Global Deluge of Initiatives Regulating AI

- European Union: LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (April 21, 2021)

- United States: National Defense Authorization Act for 2021
  - Directs NIST to develop "a voluntary risk management framework for trustworthy AI systems"

- United States: National AI Initiative Act of 2020 Mandate to Department of Commerce
  - Department of Commerce establishes National Artificial Intelligence Advisory Committee (NAIAC) September 2021

Global Deluge of Initiatives Regulating AI

- United States: Federal Trade Commission Memorandum: "Aiming for truth, fairness, and equity in your company's use of AI" (April 2021)
  - FTC will enforce against *biased algorithms* under:
    - Article 5 Authority to regulate unfair trade practices
    - Fair Credit Reporting Act (FCRA)
    - Equal Credit Opportunity Act (ECOA)

- United States: Food and Drug Administration
  - Food & Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan

- National Security Commission on Artificial Intelligence (NSCAI) Final Report to Congress

- California Privacy Rights Act – Profiling Now Regulated

Challenges For the AI Sector

- Competing Regulatory Schemes and Approaches
  - EU using "Heavy Stick" model similar to GDPR
    - Aggressive extraterritorial reach
      - Requires appointment of Designated Representative in EU for importers of AI software
    - Establishes European Artificial Intelligence Board (similar approach to European Data Protection Board – EDPB) proscriptive approach
  - Jaw-dropping penalties – the *higher* of
    - 30 000 000 EUR
    - 6 % of worldwide annual turnover
  - US: various agencies competing for authority
    - Stakeholder participation, if any, varies according to regulatory authority
  - Virtual guarantee of inconsistent process and outcomes

What To Do?

- Assume the strictest regulatory common denominator
  - Almost certain to be European Union
  - Will become effective *before* any meaningful US initiatives
  - More comprehensive process – *spans all sectors*
  - Key objectives of EU proposed regulation arguably laudatory
    - ensure legal certainty
    - provide the flexibility to accommodate future technological developments
  - US Federal regulators increasingly active, but siloed
    - Patchwork quilt of sectoral federal regulations that cross over multiple sectors
  - States also regulating: CPRA directs California AG to develop regulations
    - Consumer access to the logic involved
    - Description of the likely outcome of the process

Basic Steps to Prepare for (More) AI Regulation

- Assess whether your *software* meets the definition of AI

    EU defines as: "software that is developed with one or more of the techniques and approaches listed in Annex 1 and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."

- Machine learning approaches, including supervised, unsupervised and reinforcement learning, using a wide variety of methods including deep learning;

- Logic- and knowledge-based approaches, including knowledge representation, inductive (logic) programming, knowledge bases, inference and deductive engines, (symbolic) reasoning and expert systems;

- Statistical approaches, Bayesian estimation, search and optimization methods.

- *Implicitly Excluded:*
  - Hardware
  - Basic software tools use to develop AI which do not meet the definition of AI

Basic Steps to Prepare for (More) AI Regulation

- Assess whether you are a "provider" or a "user"

    Provider: "a natural or legal person, public authority, agency or other body that develops an AI system or that has an AI system developed with a view to placing it on the market or putting it into service *under its own name or trademark*, whether for payment or free of charge"

    User: "any natural or legal person, public authority, agency or other body using an AI system under its authority, except where the AI system is used in the course of a personal non-professional activity"

    Not covered?: B2B supply chain unbranded software

Basic Steps to Prepare for (More) AI Regulation

Understand Your Risk Category

- Prohibited
- High Risk
- Limited Risk
- Minimal risk

Prohibited

- Systems whose use is considered unacceptable as contravening European Union values, (for instance by violating fundamental rights)
  - deploy subliminal techniques beyond a person's consciousness
  - exploit vulnerabilities of specific groups of people to materially distort behavior in a manner that causes or is likely to cause physical or psychological harm
  - used by public authorities to score and classify people
  - use real-time remote biometric identification in public spaces for law enforcement purposes

High Risk

- Biometric Identification (real time or "post" real time)

- Management and Operation of Critical Infrastructure

- Determining access, assigning, or assessing persons in the context of educational or vocational training or admission testing

- Evaluating an individuals' creditworthiness

- Using AI systems in recruitment and promotion (including changes to roles and responsibilities) in an employment context

- Access to or enjoyment of essential public or private services

- Migration, asylum and border control management

- AI systems to assist a judicial authority in researching and interpreting facts and the law and in applying the law to a concrete set of facts

High Risk – Law Enforcement

- Making individual risk assessments of natural persons in order to assess the risk of a natural person for offending or reoffending

- Used by law enforcement authorities as polygraphs and similar tools or to detect the emotional state of a natural person

- AI systems intended to be used by law enforcement authorities to detect deep fakes

- AI systems intended to be used by law enforcement authorities to detect deep fakes

- AI systems for predicting the occurrence or reoccurrence of an actual or potential criminal offence based on profiling or assessing personality traits and characteristics or past criminal behavior of natural persons or groups

Unique Aspects Regarding Biometrics

- Biometric Identification System defined functionally:
  - AI system intended for the identification of natural persons at a distance through the comparison of a person's biometric data with the biometric data contained in a reference database, and without prior knowledge whether the targeted person will be present and can be identified, irrespectively of the particular technology, processes or types of biometric data used

- Distinguishes between 'real-time' and 'post' remote biometric identification systems
  - Both categorized as high risk
  - Real time relatively greater risk, more safeguards required

Limited-Minimal Risk Obligations

- Informing users when they interact with an AI system such as chatbots or their emotions or characteristics are recognized through automated means; and

- Informing individuals that content has been generated through automated means if an AI system creates "deep fakes" by manipulating image, audio, or video content that resembles authentic content:
  - If an AI system is used to generate or manipulate image, audio or video content that appreciably resembles authentic content, there should be an obligation to disclose that the content is generated through automated means, subject to exceptions for legitimate purposes (law enforcement, freedom of expression in the arts and sciences)

Clear Intent to Regulate *Outside* EU

- Operator established in the Union that contracts certain services to an operator established outside the Union in relation to an activity to be performed by an AI system that would qualify as high-risk and whose effects impact natural persons located in the Union

- Appl[ies] to providers and users of AI systems that are established in a third country, to the extent the output produced by those systems is used in the Union.

Documentation Is Critical

- Impossible to predict precise contours of regulations

- Cannot wait (years!) for the regulations to become final

- Demonstrate good faith efforts to understand and comply with regulatory objectives (the spirit of the law) even if the letter of the law is yet to come

Data Set Accuracy

- Core focus of EU Proposed Regulation

    High data quality is essential for the performance of many AI systems, especially when techniques involving the training of models are used, with a view to ensure that the high-risk AI system performs as intended and safely and it does not become the source of discrimination prohibited by EU law

    ***

    Training, validation and testing data sets require the implementation of appropriate data governance and management practices

- FTC

    Training, validation and testing data sets require the implementation of appropriate data governance and management practices

AI Regulation is More About _Process_ Than Proscription

- Regulators appreciate that AI will continue to evolve; proscribing rigid regulations (exception: prohibited categories) would be fruitless
  - EU asserts its intent is to be innovation friendly"
  - EU's express reference to "Future-proofing " (nowhere defined?) in the recitals implicitly acknowledges the speed of innovation in this space

- _Burden is being shifted_ to the regulated community

- _Documenting_ your processes for assessing risks will be critical

- You don't have to be perfect, but you need to be able to tell your story
  - "Here are the facts, and risks, as we believed them to be"
  - "This is the process we used to minimize and mitigate those risks"
  - "This is the continuous improvement process we used"

Resources

- European Union: LAYING DOWN HARMONISED RULES ON ARTIFICIAL INTELLIGENCE (April 21, 2021)

https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0206&from=EN

- **United States: National Defense Authorization Act for 2021**

- https://www.law.com/njlawjournal/2022/04/08/artificial-intelligence-and-you-perfect-together/

- United States: National AI Initiative Act of 2020 Department of Commerce establishes National Artificial Intelligence Advisory https://www.commerce.gov/news/press-releases/2021/09/department-commerce-establishes-national-artificial-intelligence

Resources

- United States: Federal Trade Commission Memorandum: "Aiming for truth, fairness, and equity in your company's use of AI" (April 2021) https://www.ftc.gov/business-guidance/blog/2021/04/aiming-truth-fairness-equity-your-companys-use-ai

- United States: Food and Drug Administration
  - Food & Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action Plan https://www.fda.gov/media/145022/download

- National Security Commission on Artificial Intelligence (NSCAI) Final Report to Congress https://www.nscai.gov/2021-final-report/