

# AI AND REGULATION: The Broader Picture



Carl Schonander/Senior Vice President – Global Public Policy  
Software & Information Industry Association (SIIA)

[cschonander@siia.net](mailto:cschonander@siia.net)

July 16, 2019/WIPO “International Conference on AI – Emerging Technologies and Intellectual Property –  
Connecting the Bits,” Tel Aviv, Israel

# But First: A Word About SIIA



AM&P, a division of  
Connectiv, The Business  
Information Association





# SIIA Public Policy



# What Should You Get Out of This Presentation?

- A sense for what is happening in the United States and internationally
- Where regulation might first impact AI
- How intellectual property is impacted

# Resources

- [SIIA Issue Brief: Ethical Principles For Artificial Intelligence And Data Analytics, 2017](#)
- [SIIA Issue Brief: New Economic Policy Research On Artificial Intelligence And The Future Of Work, 2017](#)
- [SIIA Issue Brief: Algorithmic Fairness, 2016](#)
- [SIIA Issue Brief: Artificial Intelligence And The Future Of Work, 2016](#)

# What is Artificial Intelligence (AI)?

## Why Does it Matter?

AI technologies and systems are considered to comprise of software and/or hardware that can learn to solve complex problems, make predictions or undertake tasks that require human-like sensing (such as vision, speech, and 51 touch), perception, cognition, planning, learning, communication, or physical action.

- AI assistants
- computer vision systems
- biomedical research
- unmanned vehicle systems
- advanced game-playing software
- facial recognition systems
- AI in both Information Technology 55 (IT) and Operational Technology (OT).

From: [NIST](#) “U.S. Leadership in AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools”

# How Did We Get Here?

ALGORITHMS JUST GETTING BETTER!

- backpropagation
- Generative Adversarial Nets (GANs)
- Long Short Term Memory Networks
- Deep Q Learning

# Potential Impact of 5G

- Actually 5G will be a huge [enabler](#) of AI...
- Quite a bit [written](#) about how AI and 5G can enable applications “at the edge” – think autonomous vehicles. Note that storing sensitive data “at the edge” could have positive privacy/security implications.

# Where Are We Going?

- Three new reports combine to suggest these answers:
  - It can probably do less right now than you think.
  - It will eventually do more than you probably think, in more places than you probably think, and will probably evolve faster than powerful technologies have in the past.

- Steve Lohr, [NYT](#), November 30, 2017

# Impact On Jobs Unclear

➤ Frey/Osborne [prediction](#):

➤ 47% of jobs can be automated does not mean that they will be

# How is the World Regulating AI?

- For the time being, there is a lot of “soft law,” especially with respect to AI and Ethics.
- AI OECD AI [Principles](#). – 5 Complementary Values-Based Principles for Responsible Stewardship of Trustworthy AI
  1. AI should benefit people and the planet by driving inclusive growth, sustainable development and well-being.
  2. AI systems should be designed in a way that respects the rule of law, human rights, democratic values and diversity, and they should include appropriate safeguards – for example, enabling human intervention where necessary – to ensure a fair and just society.
  3. There should be transparency and responsible disclosure around AI systems to ensure that people understand AI-based outcomes and can challenge them.
  4. AI systems must function in a robust, secure and safe way throughout their life cycles and potential risks should be continually assessed and managed.
  5. Organisations and individuals developing, deploying or operating AI systems should be held accountable for their proper functioning in line with the above principles.

# OECD AI Principles

## **1.3. Transparency and explainability**

AI Actors should commit to transparency and responsible disclosure regarding AI systems. To this end, they should provide meaningful information, appropriate to the context, and consistent with the state of art:

- i. to foster a general understanding of AI systems,
- ii. to make stakeholders aware of their interactions with AI systems, including in the workplace
- iii. to enable those affected by an AI system to understand the outcome, and,
- iv. to enable those adversely affected by an AI system to challenge its outcome based on plain and easy-to-understand information on the factors, and the logic that served as the basis for the prediction, recommendation or decision.

# OECD Principles Continued

## **1.4. Robustness, security and safety**

- a) AI systems should be robust, secure and safe throughout their entire lifecycle so that, in conditions of normal use, foreseeable use or misuse, or other adverse conditions, they function appropriately and do not pose unreasonable safety risk.
- b) To this end, AI actors should ensure traceability, including in relation to datasets, processes and decisions made during the AI system lifecycle, to enable analysis of the AI system's outcomes and responses to inquiry, appropriate to the context and consistent with the state of art.
- c) AI actors should, based on their roles, the context, and their ability to act, apply a systematic risk management approach to each phase of the AI system lifecycle on a continuous basis to address risks related to AI systems, including privacy, digital security, safety and bias.

# OECD Principles Continued

## **1.5.Accountability**

AI actors should be accountable for the proper functioning of AI systems and for the respect of the above principles, based on their roles, the context, and consistent with the state of art.

# United States Strategy

The National Artificial Intelligence Research and Development [Strategic Plan](#): 2019 Update.

- 1) Long-term investments
- 2) Human-AI collaboration
- 3) Ethical, legal, and societal issues
- 4) Safety and security
- 5) Shared public datasets for training/testing
- 6) Standards and benchmarks
- 7) Workforce needs
- 8) Public/Private Partnerships

# Strategy 3 Is of Greatest Interest

- DARPA Explainable AI (XAI) program – create a suite of ML techniques that produce more explainable AI systems while maintaining high level of learning performance (prediction accuracy)
- NSF and Amazon working on research focused on AI fairness

# Strategy 3 Continued

How can architectures for ethical AI be designed?

- Two-tier monitor architecture that separates operational AI from a legal/ethics assessment agent
- Safety engineering overseen by assessment agency – agent is actually overseeing the engineering
- Ethical architecture using set theoretic principles, combined with logical constraints on AI system behavior that restrict action to conform to ethical doctrine

# Standards Are Key for Operationalization

[NIST Draft Plan](#) for Federal Engagement in AI Standards Development is Important

- Everything in the plan is important but prioritization needed.
- Tools for accountability and auditing (algorithmic transparency) really important. Working on this internationally crucial. Make this applicable across sectors.
- Reinforce point that ethics considerations should be tied to risk to humans.
- Privacy should indeed be incorporated into standards for PII AI applications.
- Support all forms of collaborative models for standards development, including open source and Federal open data, consistent with respect for the contribution that private sector proprietary models can also make.
- Increase data discoverability and access to Federal government data.

# Tools Are Also Needed

- Lots of different tools needed.
- Policymakers likely to focus on tools for accountability and auditing to enable examination of an AI system's output, including traceability, to provide a record of events such as their implementation, testing, and completion.

# EU High-Level Expert Group on AI

[Ethics Guidelines](#) – Seven Steps to Achieve “Trustworthy AI”

1. Human agency and oversight
2. Technical robustness and safety
3. Privacy and data governance
4. Transparency
5. Diversity, non-discrimination and fairness
6. Societal and environmental wellbeing
7. Accountability

# High-Level Expert Group Continued

## Expert Group [Policy Recommendations](#)

- *Where an AI-based service does not run properly or when an individual so requests, he or she should be able to interact with a human interlocutor, when there is a significant impact on the individual.*
- *Set up a single point of contact for individuals, for example by deploying natural user interfaces that can redirect individuals to the sought after information or service in an easily accessible*
- *Develop tools to ensure that public services can be deployed for all, and in a manner that safeguards individuals' fundamental rights, democracy and the rule of law.*

# International AI Approaches

- Elliott School of International Affairs “Digital Trade and Data Governance [Hub](#).”
- Lists and provides some detail on Argentina, Australia, Brazil, Canada, China, France, Germany, EU, India, Japan, Kenya, Mexico, South Korea, UK and US AI plans/strategies.

# How Should We Regulate AI?

- Be Domain-Specific!
- Recognize there are many different applications of AI.

# Examples of Applications

See this [piece](#) on 11 different applications.

- **Artificial Narrow Intelligence, “weak AI”** – one task at a time. E.g. Siri or Bixby.
- **Artificial General Intelligence, “strong AI”** – no real applications now.
- **Big data** – derives info. from data too complex for standard data analysis. E.g. Netflix.
- **Computer vision** – processing of visual images. E.g. images that Tesla cars see.
- **Data mining** – sorting thru large sets of data. E.g. Amazon analysis of purchases.
- **Machine Learning** – machines learning without being explicitly being programmed. E.g. Targeted ads on social media, virtual voice assistants on cell phones, facial recognition software on social media websites, Google Maps or cellphone GPS data.
- **Deep Learning** – teaching computers how to learn by rote. E.g. Avs and VAs.
- **Convolutional neural networks** – analysis of visual network using multilayer perceptions. E.g. identification of objects within scenes.
- **Generative adversarial networks** – networks that can generate seemingly authentic photos.
- **Natural language processing** – analysis of language. E.g. speech-to text conversion of VMs.

# Examples of AI Impact On Law, Regulation, Trade Agreements

- Automated Decisionmaking And Explainability
- Bias/Transparency
- Text And Data Mining

# “Conflation” is an Issue

- Artificial Intelligence and Automated Decisionmaking are often conflated.
  - In the United States, this often means dealing with questions of bias.
  - In the EU, it is all about how to comply with the GDPR’s rules on automated decisionmaking.

# Take A Look At The GDPR

- GDPR's [Article 22](#).
  - The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.
  - Paragraph 1 shall not apply if the decision:
    - is necessary for entering into, or performance of, a contract between the data subject and a data controller;
    - is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or
    - is based on the data subject's explicit consent.
  - In the cases referred to in points (a) and (c) of paragraph 2, the data controller shall implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the controller, to express his or her point of view and to contest the decision.
  - Decisions referred to in paragraph 2 shall not be based on special categories of personal data referred to in [Article 9](#)(1), unless point (a) or (g) of [Article 9](#)(2) applies and suitable measures to safeguard the data subject's rights and freedoms and legitimate interests are in place.

# Article 22 Needs to be Read Together with Recital 71

## [Recital 71](#)

The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. <sup>2</sup>Such processing includes ‘profiling’ that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject’s performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. <sup>3</sup>However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. <sup>4</sup>In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. <sup>5</sup>Such measure should not concern a child.

In order to ensure fair and transparent processing in respect of the data subject, taking into account the specific circumstances and context in which the personal data are processed, the controller should use appropriate mathematical or statistical procedures for the profiling, implement technical and organisational measures appropriate to ensure, in particular, that factors which result in inaccuracies in personal data are corrected and the risk of errors is minimised, secure personal data in a manner that takes account of the potential risks involved for the interests and rights of the data subject, and prevent, inter alia, discriminatory effects on natural persons on the basis of racial or ethnic origin, political opinion, religion or beliefs, trade union membership, genetic or health status or sexual orientation, or processing that results in measures having such an effect. <sup>7</sup>Automated decision-making and profiling based on special categories of personal data should be allowed only under specific conditions.

# Report On Automated Decision-Making in the EU

See this AlgorithmWatch [Report](#).

## ***“Why automated decision-making instead of Artificial Intelligence?”***

“One of the first hard questions to answer is that of defining the issue. We maintain that the term automated decision-making (ADM) better defines what we are faced with as societies than the term ‘Artificial Intelligence’, even though all the talk right now is about ‘AI’. Algorithmically controlled, automated decision-making or decision support systems are procedures in which decisions are initially—partially or completely—delegated to another person or corporate entity, who then in turn use automatically executed decision-making models to perform an action. This delegation—not of the decision itself, but of the execution—to a data-driven, algorithmically controlled system, is what needs our attention. In comparison, Artificial Intelligence is a fuzzily defined term that encompasses a wide range of controversial ideas and therefore is not very useful to address the issues at hand. In addition the term ‘intelligence’ invokes connotations of a human-like autonomy and intentionality that should not be ascribed to machine-based procedures. Also, systems that would not be considered Artificial Intelligence by most of today’s definitions, like simple rulebased analysis procedures, can still have a major impact on people’s lives, i.e. in the form of scoring systems for risk assessment.”

# United States:

## Focus is on Bias And Explainability

See below for Laws which are applicable to AI/Automated Decisionmaking

- Fair Credit Reporting Act (FCRA)
- Civil Rights Act
- Equal Credit Opportunity Act
- Age Discrimination in Employment Act
- Genetic Information Nondiscrimination Act
- Affordable Care Act

# Senators Wyden-Booker Proposal

- Senators Wyden and Booker have proposed the “Algorithmic Accountability [Act](#) of 2019.”
- Note the special rules for “high-risk automated decision making systems” and “high risk information systems”

# What Should Companies Do?

- Consider seeking out affirmative ways to use data analytics to ensure fairness, as illustrated by the use of alternative credit scores to improve the credit granting process for historically underserved groups, and the ways in which data analytics can detect/remedy bias.
- Recognize that the current U.S. framework of non-discrimination and consumer protection law applies to the use of big data analytics. Companies need to have adequate resources devoted to compliance with current law.
- Consider how to provide an indication of the kinds of factors that go into decision-making algorithms.
- Conduct internal assessments both at the design stage and as algorithms are actually employed in practice. The methods developed for disparate impact analysis used under current law provides a guide for doing this. A number of issues related to assessments need to be addressed including the metrics used, the circumstances under which it makes sense to conduct them, and the role of different stakeholders, including outside researchers, who could provide valuable guidance on the methodologies for internal assessments. It is important to focus these efforts on uses that create consequential impacts on people's lives and where there is a significant risk for individual or societal harm.
- Develop standards of fairness to guide company actions in response to their internal assessments. In particular, firms should understand the extent to which they are aiming at accuracy in prediction and the extent to which they are seeking to prevent disproportionate adverse impacts on protected groups. These standards will help to guide their actions in response to any findings of disparate impact.

# Text and Data Mining

- It is all about the data! TDM a big issue in EU Copyright Directive – See [Articles 3 and 4.](#)
- Relevant to AI given AI need for data. Our view.
  - implement language faithfully
  - recall it is right of reproduction, not communication to the public
  - security critical
  - engage in best practices
- Important to maintain incentives for data curation.

# Trade Agreements

United States Mexico Canada Agreement builds on TPP. See [Article 19.16](#).

## **Article 19.16: Source Code**

1. No Party shall require the transfer of, or access to, a source code of software owned by a person of another Party, or to an algorithm expressed in that source code, as a condition for the import, distribution, sale or use of that software, or of products containing that software, in its territory.
2. This Article does not preclude a regulatory body or judicial authority of a Party from requiring a person of another Party to preserve and make available the source code of software, or subject to safeguards against unauthorized disclosure.

# Lessons

- Plenty of soft law being developed around the world.
- Hard law coming first in algorithmic transparency/decisionmaking and privacy.
- AI developers use all kinds of IPRs to protect their rights.
  - In the AI context, at this time, protections for algorithms and source code coming thru trade agreements in the sense that USMCA and TPP prevent mandatory disclosure as a condition for doing business.

# Be on the Lookout for Unexpected Law and Regulation!

- Best example is French ban on the use of judicial analytics. I wrote about this [here](#).
- The law bans the use of analytics tools to analyze French court decisions.
- Note that at least in the United States, the discussion has been about the application of algorithms by courts. This bans the use of AI to analyze court decisions.

THE END