Comments on "White Paper on Artificial Intelligence: a European approach to excellence and trust"

June 10, 2020
AI Utilization Strategy Task Force
Committee on Digital Economy
Keidanren

1. Overview

The AI White Paper[1] released recently by the European Commission deals with both AI innovation by a broad range of entities, including small and mid-sized enterprises, and building an "ecosystem of trust" for the utilization of AI. This is in line with Keidanren's goal of building a "Trusted Quality AI Ecosystem."

However, the European Commission uses a very broad definition of its envisioned AI, encompassing AI systems using deep learning and other forms of machine learning, AI based on symbol manipulation, as well as a broad range of information systems beyond the bounds of AI, such as technologies combining data, algorithms, and computing power whose reasoning process is not a "black box." While the difficulty of defining AI is understandable, careful thought still needs to be given to its definition since no entity has yet succeeded in coming up with a widely accepted precise definition.

AI technology and business are still in the development phase. It is necessary to prioritize discussions with the stakeholders and promotion of greater sharing of efficient processes and technologies in order to come to a broad common understanding. The White Paper needs to state that hasty regulation runs the risk of obstructing the utilization of AI and business activities in society.

The necessary tools cannot be maintained and social benefits may be undermined unless the following goals can all be achieved: rapid technological innovation, which characterizes the AI fields; finding an optimal balance in human rights by both safeguarding people's privacy

[1] White Paper on Artificial Intelligence: a European approach to excellence and trust（released on Feb. 19, 2020）

and ensuring people's day-to-day livelihoods, safety, and health, an issue that has emerged amid the COVID-19 crisis; and ensuring the profitability of business activities. As well as looking for ways to institute balanced regulations, we hope that discussions from now on will lead to the compatibility of future standards and regulations, mutual recognition of labeling, and such other matters relating to building coherent and compatible AI ecosystems.

２． Specific Points

Page 7 E. PARTNERSHIP WITH THE PRIVATE SECTOR

Page 7, last paragraph

"Action 5: In the context of Horizon Europe, the Commission will set up a new public private partnership in AI, data and robotics to combine efforts, ensure coordination of research and innovation in AI, collaborate with other public-private partnerships in Horizon Europe and work together with the testing facilities and the Digital Innovation Hubs mentioned above."

Our comment

- Collaboration between Japan and the EU giving full play to their strengths will contribute to the promotion of AI innovation. Consideration of cooperation with the Japanese government, research organizations, and industry in Horizon Europe should be accelerated.

Page 8 G. SECURING ACCESS TO DATA AND COMPUTING INFRASTRUCTURE

Page 8, paragraph 3

"Promoting responsible data management practices and compliance of data with the FAIR principles will contribute to build trust and ensure re-usability of data. Equally important is investment in key computing technologies and infrastructures."

Our comment

- In view of the importance of management and compliance systems that will facilitate the utilization of data while also protecting privacy and securing individual rights, concrete steps for "responsible data management" should be considered based on discussions under various international frameworks.

Page 8 H. INTERNATIONAL ASPECTS

Page 8, last paragraph–page 9, first paragraph

"The EU will continue to cooperate with like-minded countries, but also with global players, on AI, based on an approach based on EU rules and values… The Commission is convinced that international cooperation on AI matters must be based on an approach that promotes the respect of fundamental rights, including human dignity, pluralism, inclusion, non-discrimination and protection of privacy and personal data26 and it will strive to export its values across the world."

Our comments

- We hope for more in-depth discussions by the OECD and other like-minded nations toward the establishment of international rules on AI development and utilization that will ensure the promotion of innovation. We also hope that national leaders will reach a consensus on this at the G20 and other international frameworks, taking into account the realities and values in each region.

- Since AI technology continues to evolve, it is not desirable to apply today's standards to future AI technology. Inasmuch as there will be ambiguities in specific regulations, we ask that the EU heed the opinions of non-EU businesses before these regulations go into force and become legally binding and provide opportunities for reviewing them based on such opinions.

Page 9 5. AN ECOSYSTEM OF TRUST: REGULATORY FRAMEWORK FOR AI

(Overall)

Our comments

- AI is simply a tool, so it is inappropriate to think of AI itself as high-risk. The technology itself does not constitute any risk; risks are brought about by how this technology is used and its users. It is more appropriate to define "high-risk applications" and "high-risk users." Furthermore, it is necessary to promote a correct understanding and enhance ethical awareness for the proper use of this tool in order to prevent the emergence of high-risk operations and users. Since the social environment will also undergo radical changes with technological innovation, regulation is not only impractical for private businesses, but may also impede the regulators' ability to adapt to future technological advances. It is premature to define and regulate high-risk AI at this point.

- The definition of high-risk AI may cause the withering of technological development in the defined areas. It is also important to take into account not only the potential damages that may arise from AI, but also the potential social losses resulting from the erosion of benefits that AI would have brought due to regulation. Excessive regulation could become an obstacle to innovation that contributes to the development of industries and the resolution of social issues in Europe. Therefore, what should be defined at this point are not regulations but rather guidelines.

- When introducing regulations in the future, this should be premised on a process consisting of closer and thorough dialogue with the industrial sector, pilot projects conducted prior to actual introduction, and thorough risk assessment. Regulation should only be limited to AI that generates truly serious risks while also ensuring legal stability and predictability.

- Since the definition of risk and the thinking on accountability are different for each sector, it is desirable for each sector to consider this issue based on their own thinking after the basic thinking applying to all sectors is presented.

- With regard to the definition and standards of risk, it is desirable to engage in a comprehensive exchange of views, not only by the EU nations, but also involving a broad range of stakeholders, including governments and industrial sectors of other countries, with an eye on a global consensus and standardization in the future.

- It is desirable not to simply focus on the introduction and review of regulations but to undertake a comprehensive gap analysis first before considering the introduction and review of regulations as an option.

Page 16 C. SCOPE OF A FUTURE EU REGULATORY FRAMEWORK

Page 17, paragraph 3

"A risk-based approach is important to help ensure that the regulatory intervention is proportionate."

Our comment

- A risk-based approach is indeed important. However, for the sake of technological advancement, a scheme for trial operation under a certain extent of oversight should also be considered in cases where AI utilization deemed to be high-risk is also an extremely high-performance system.

Page 17, paragraph 3

"The determination of what is a high-risk AI application should be clear and easily understandable and applicable for all parties concerned."

Our comment

- When considering the definition of high-risk AI in the future, there need to be thorough prior discussions on risk assessment by diverse stakeholders, and the definition of "high risk" must only be applied to AI that carries truly serious risks. As stated in the White Paper, it is necessary to ensure legal stability and predictability through a clear determination of what constitutes high risk.

Page 18 D. TYPES OF REQUIREMENTS

(Overall)

Our comment

- The requirements in (a)–(f) need to be fair, reasonable, and realistic. The standards need to be clear and their reasoning and appropriateness explicit in order to enhance legal stability and predictability. Furthermore, it is also necessary to review these standards as appropriate to keep in step with technological advancement.

Page 18 a) Training data

Page 19, paragraph 2

"For instance, requirements ensuring that AI systems are trained on data sets that are sufficiently broad and cover all relevant scenarios needed to avoid dangerous situations."

Page 19, paragraph 3

"These requirements could entail in particular obligations to use data sets that are sufficiently representative, especially to ensure that all relevant dimensions of gender, ethnicity and other possible grounds of prohibited discrimination are appropriately reflected in those data sets."

Our comment

- While it is indeed important to give consideration to "data sets that are sufficiently broad and cover all relevant scenarios," it is difficult to define its scope clearly. Therefore, it is not realistic to set requirements for training data that will guarantee the prevention of crisis. At the same time, it is also unrealistic to set "obligations to use data sets that are sufficiently representative" since it is difficult to define "data sets that are sufficiently representative." Careful discussion is needed in this respect.

Page 19, paragraph 3

"Requirements to take reasonable measures aimed at ensuring that such subsequent use of AI systems does not lead to outcomes entailing prohibited discrimination. These requirements could entail in particular obligations to use data sets that are sufficiently representative, especially to ensure that all relevant dimensions of gender, ethnicity and other possible grounds of prohibited discrimination are appropriately reflected in those data sets."

Our comments

- Although it is very important to use unbiased data sets to avoid discrimination generated by AI, in practice, the use of biased data sets is unavoidable. The use of unbiased data sets should only be a recommendation, and in cases where the original data is biased, use of the data should be allowed if the bias is mitigated by algorithms and other means.

- Since fairness in data sets has not been defined at this point, it is necessary to examine its definition and margin of tolerance.

Page 19 b) Keeping of records and data

Page 19, last paragraph–page 20 paragraph 1

“The records, documentation and, where relevant, data sets would need to be retained during a limited, reasonable time period to ensure effective enforcement of the relevant legislation. Measures should be taken to ensure that they are made available upon request, in particular for testing or inspection by competent authorities.”

Our comments

- Data retention is basically necessary from the standpoint of providing proof of safety and traceability during audits. On the other hand, algorithms and the development of AI applications are the results of long-term R&D of companies. Therefore, it is necessary to pay attention to the cost of record keeping for all data sets used and the difficulty of compliance with privacy rules in EU and elsewhere (for instance, rules on deleting personal information when no longer needed).

- Documents, training methods, processes, and technology for the building, testing, and validation programs of AI systems are confidential information held by each company and they should not be asked to provide such information without cause. If government authorities seek to obtain such information, a clear reason for doing so should be provided. Appropriate procedures should also be followed, such as limiting the information sought to the minimum required and careful handling of confidential information.

Page 20 c) Information provision

Page 20, paragraph 4

"Ensuring clear information to be provided as to the AI system's capabilities and limitations, in particular the purpose for which the systems are intended, the conditions under which they can be expected to function as intended and the expected level of accuracy in achieving the specified purpose."

Our comment

- It is difficult to explain in terms comprehensible to humans the "capabilities and limitations" of recent AI systems using complex models to enhance sophistication based on deep learning. Therefore, information and methods necessary for human comprehension should be provided.

Page 20 d) Robustness and accuracy

Page 20, paragraph 6

"AI systems – and certainly high-risk AI applications – must be technically robust and accurate in order to be trustworthy. That means that such systems need to be developed in a responsible manner and with an ex-ante due and proper consideration of the risks that they may generate. Their development and functioning must be such to ensure that AI systems behave reliably as intended. All reasonable measures should be taken to minimise the risk of harm being caused."

Our comment

- Technical guarantee of the "robustness and accuracy of AI systems" is of vital importance for users to use AI systems with peace of mind, but at this point, this is not possible in reality. Therefore, excessive demands such as total protection from external attacks must not be made on businesses. Instead, realistic measures, including early detection of external attacks and minimization of impact on the system, should be required.

Page 20, paragraph 9

"Requirements ensuring that outcomes are reproducible"

Our comment

- It must be noted that depending on the type of algorithms used, the results may not be fully reproducible in *ex post* verification in certain cases, such as when AI systems use random numbers in the learning process.

Page 20, last paragraph

"Requirements ensuring that AI systems can adequately deal with errors or inconsistencies during all life cycle phases"

Our comment

- It must be noted that there are cases where AI systems carry out further learning and evolve further using data obtained after the sale of the product, rendering it difficult to provide advance guarantee that errors and inconsistencies throughout the product cycle can be dealt with properly.

Page 21 e) Human oversight

Page 21, paragraph 2

"Human oversight helps ensuring that an AI system does not undermine human autonomy or cause other adverse effects. The objective of trustworthy, ethical and human-centric AI can only be achieved by ensuring an appropriate involvement by human beings in relation to high-risk AI applications."

Our comments

- Although human oversight and appraisal of AI is important, excessive human involvement may delay the application of AI and impede innovation when the expansion of AI applications, including IoT and M2M, is expected. Therefore, the level of human involvement and the areas where this is applicable should be considered carefully.

- It is better to waive the requirement for human oversight when AI's self-verification of its actions is proven to be less biased or more accurate than human verification. Furthermore, when this requirement applies, practical oversight conditions should be set.

Page 21, paragraph 7

"in the design phase, by imposing operational constraints on the AI system (e.g. a driverless car shall stop operating in certain conditions of low visibility when sensors may become less reliable or shall maintain a certain distance in any given condition from the preceding vehicle)."

Our comments

- Design should be based on the assumption that breakdowns and malfunctioning could occur, and it is necessary to build in mechanisms and operational principles for safety control. Particularly in the design of high-precision AI realized with extremely complicated models, full consideration also needs to be given to subsequent scenarios.

- If the overall AI system has built-in designs for risk elimination, the requirement for human oversight should be waived.

Pages 18, 21 f) Specific requirements for remote biometric identification

Page 18

"Note 52 Remote biometric identification should be distinguished from biometric authentication... Remote biometric identification is..."

Page 21, last paragraph

"The gathering and use of biometric data for remote identification purposes, for instance through deployment of facial recognition in public places, carries specific risks for fundamental rights."

Our comments

- The scope of definition and use of remote biometric identification and biometric authentication, as well as the difference between the two are unclear. These should be clarified by citing examples, for instance.

- Face recognition in public places, in particular, has great potentials for use in immigration procedures, anticrime measures, and other public welfare purposes. Therefore, the uniform regulation of face recognition for public use, even in cases where individual consent cannot be obtained, should be avoided.

- Use of face recognition in the private sector with the individual's consent should proceed based on the views of diverse stakeholders and with due consideration for privacy, in order not to restrict its utilization in the private sector unnecessarily.

- The definition of remote biometric identification, biometric authentication, and so forth, including their scope and use, is unclear. A legal system has yet to be established to govern the use of biometric data, such as face recognition and fingerprint data. For this reason, it is necessary to come up with a clear definition and engage in careful discussions when formulating regulations on remote biometric identification, in order not to overly restrict private sector utilization.

- Furthermore, when it is necessary to respond to public health crises, regulations that give full consideration to privacy but hinder the achievement of public welfare goals to protect people's lives are undesirable.

Page 22, paragraph 4

"… the Commission will launch a broad European debate on the specific circumstances, if any, which might justify such use, and on common safeguards."

Our comment

- It is necessary to heed the views of multiple stakeholders and proceed with the discussion with a firm grasp of the risks of using AI for biometric identification in public places.

Page 22 <u>E. Addressees</u>

Page 22, paragraph 7

"For example, while the developers of AI may be best placed to address risks arising from the development phase, their ability to control risks during the use phase may be more limited. In that case, the deployer should be subject to the relevant obligation… Under EU product liability law, liability for defective products is attributed to the producer, without prejudice to national laws which may also allow recovery from other parties."

Our comments

- While it says here that “the deployer should be subject to the relevant obligation,” the development of AI systems and products and services using AI involve multiple organizations and responsible persons in most cases. For this reason, it is necessary to define “providers” and other entities, delineate the scope of accountability of each entity specifically, and clarify the definition and scope of “defects.”

- Responsibility should not lie solely on the developers and AI service providers. A balance with the obligation of the service recipients and other entities should also be considered.

Page 23 F. Compliance and Enforcement

Our comment

- It is necessary to clarify the subjects and standards of prior conformity assessment in order to enhance legal stability and predictability.

Page 23, paragraph 2

“In view of the high risk that certain AI applications pose for citizens and our society (see section A above), the Commission considers at this stage that an objective, prior conformity assessment would be necessary to verify and ensure that certain of the above mentioned mandatory requirements applicable to high-risk applications (see section D above) are complied with.”

Note 59

“The system would be based on conformity assessment procedures in the EU… See the Blue guide on the Implementation of EU product rules, 2014. ”

Our comments

- Excessive prior conformity assessment may impede the marketing of AI systems and innovation due to the cumbersome procedures and additional time required. It is better to set up a joint government-private sector scheme for the proper assessment of businesses' own initiatives.

- It is necessary to clarify the subjects and standards for prior conformity assessment in order to enhance legal stability and predictability. As well as clarifying the details of "existing prior conformity assessment," the contents of additional assessments to be imposed on transportation, medical equipment, and other areas requiring a high level of safety should also be clarified.

- In light of technological advancement in AI and the shortage of manpower, it is reckoned that thorough implementation of prior conformity assessment by the authorities will be extremely difficult. Self-assessment by developers and service providers should also be considered.

Page 23, paragraph 2

"It could include checks of the algorithms and of the data sets used in the development phase."

Our comment

- When the authorities implement prior conformity assessment, they should not unduly seek the disclosure of information that could be sources of competitiveness (e.g. algorithms, details of data sets). Disclosure should not include confidential information and must be limited to the minimum required, and the reason for seeking such disclosure must be clarified.

Page 23, paragraph 8

"In case the conformity assessment shows that an AI system does not meet the requirements for example relating to the data used to train it, the identified shortcomings will need to be remedied, for instance by re-training the system in the EU in such a way as to ensure that all applicable requirements are met."

Our comments

- Requiring re-training in the EU zone may lead to performance demands on foreign companies (e.g. use of local contents, technology transfer). Therefore, there should be no regulations on the methods and location of re-training when the requirements are not met.

- If prior conformity assessment shows that physical safety devices or operations can fully eliminate or reduce the risks of systems using high-risk AI, it is desirable to waive or ease all or part of the requirements corresponding to the risk elimination and reduction steps taken.

Page 24, paragraph 1

"Ex-post controls should be enabled by adequate documentation of the relevant AI application (see section E above) and, where appropriate, a possibility for third parties such as competent authorities to test such applications."

Our comment

- With regard to *ex post* investigation relating to risks posed by AI to basic rights that the authorities may conduct after AI systems are deployed, clear rules should be set for conducting such investigation to enhance businesses' predictability.

Page 24 G. VOLUNTARY LABELLING FOR NO-HIGH RISK AI APPLICATIONS

Page 24, paragraph 5

"The voluntary label would allow the economic operators concerned to signal that their AI-enabled products and services are trustworthy. It would allow users to easily recognise that the products and services in question are in compliance with certain objective and standardised EU-wide benchmarks, going beyond the normally applicable legal obligations. This would help enhance the trust of users in AI systems and promote the overall uptake of the technology."

Our comments

- In addition to labeling schemes, an approach to support industry-led moves toward global standardization, such as providing efficient technologies and processes to ensure the reliability of AI, should also be considered.

- Since it is difficult to fully enforce laws and regulations at the introduction stage of new technology, there should probably be leeway to leave this matter to self-regulation and code of conduct by businesses.

Page 25 H. Governance

Page 24, paragraph 7

"A European governance structure on AI in the form of a framework for cooperation of national competent authorities is necessary to avoid fragmentation of responsibilities, increase capacity in Member States, and make sure that Europe equips itself progressively with the capacity needed for testing and certification of AI-enabled products and services. In this context, it would be beneficial to support competent national authorities to enable them to fulfil their mandate where AI is used.

Our comments

- The governance authorities of national governments or organizations commissioned by these authorities to investigate must have adequate specialized knowledge and must implement thorough protection of confidential information provided for the investigation. Moreover, standards and subjects of investigation should be uniform in each nation.

- The EU should also consider delegating investigation powers to its members. If each nation set up their own independent regulatory authorities, it is expected that this may undermine the effectiveness and efficiency of investigations due to overlapping administration with existing agencies and inadequate complementation between the national authorities in terms of the industrial sectors' knowhow and specialized knowledge on AI. The cost of responding to such a situation may ultimately fall on the EU citizens and the end users.

Page 25, paragraph 4

"The EU enjoys excellent testing and assessment centres and should develop its capacity also in the area of AI. Economic operators established in third countries wanting to enter the internal market could either make use of designated bodies established in the EU or, subject to mutual recognition agreements with third countries, have recourse to third-country bodies designated to carry out such assessment."

- The design and renewal of testing methods and assessment regimes for the rapidly evolving AI applications should be considered in terms of human resources development and changing the assessment regimes in response to changes in AI systems, in order to achieve both precision and speed.

Page 25, paragraph 4

"The EU enjoys excellent testing and assessment centres and should develop its capacity also in the area of AI. Economic operators established in third countries wanting to enter the internal market could either make use of designated bodies established in the EU or, subject to mutual recognition agreements with third countries, have recourse to third-country bodies designated to carry out such assessment."

Our comment

- In line with the policy of allowing the use of designated third-country assessment bodies when there is a mutual recognition agreement, we hope for the expansion of mutual recognition between nations with advanced AI technology.