Recommendations from BSA | The Software Alliance on Japan's AI Strategy in the New Era of AI

May 5, 2023

General Comments

BSA | The Software Alliance (**BSA**)[1] appreciates the leadership of the Project team on Evolution and Implementation of AI (**Project Team**), launched under the Digital Society Promotion Headquarters of Liberal Democratic Party, in encouraging the Government of Japan to further accelerate AI uptake in "The AI White Paper-Japan's National Strategy in the New Era of AI" (**White Paper**). We welcome the recommendations in the White Paper, which acknowledges the need for Japan to develop a new national AI strategy focused on nurturing and strengthening AI development capacity and advancing and supporting AI utilization in the public and private sectors. We are encouraged that the Project Team fully recognizes the benefits AI can bring to improve productivity, quality, and efficiency in society. BSA appreciates and supports the approach that has been taken in Japan, as demonstrated in the "Governance Guidelines for Implementation of AI Principles" developed by the Ministry of Economy, Trade and Industry, supporting industry's voluntary efforts.[2] BSA and its members are eager to work with the Project Team and the Government of Japan to enable AI to be developed and used responsibly in support of Japan's economic growth, competitiveness, and job creation.

BSA is the leading advocate for the global software industry. Our members are at the forefront of software-enabled innovation that is fueling global economic growth, including cloud computing, data analytics, and artificial intelligence (**AI**). BSA members help societies harness the benefits of AI in every sector, transforming people's lives in incredible ways, helping them solve complex problems, and driving innovation across the globe.[3] As BSA members are leaders in the development of cutting-edge technologies, BSA has unique insights into both their tremendous potential and the government policies that can best support their responsible development and use.

While the adoption of AI provides unquestionable benefits for organizations, consumers, and society, we also recognize that if this technology is not developed and deployed responsibly, it can result in significant risks. BSA recognizes that AI can be used in harmful ways. For

[1] BSA's members include: Adobe, Alteryx, Altium, Amazon Web Services, Atlassian, Autodesk, Bentley Systems, Box, Cisco, Cloudflare, CNC/Mastercam, Dassault, Databricks, DocuSign, Dropbox, Graphisoft, IBM, Informatica, Juniper Networks, Kyndryl, MathWorks, Microsoft, Nikon, Okta, Oracle, Prokon, PTC, Rockwell, Rubrik, Salesforce, SAP, ServiceNow, Shopify Inc., Siemens Industry Software Inc., Splunk, Trend Micro, Trimble Solutions Corporation, TriNet, Twilio, Unity Technologies, Inc., Workday, Zendesk, and Zoom Video Communications, Inc.

[2] At https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20220128_2.pdf

[3] For further details, please refer to "Artificial Intelligence in Every Sector", June 13, 2022 at https://www.bsa.org/policy-filings/artificial-intelligence-in-every-sector

22F Shibuya Mark City West
1-12-1 Dogenzaka Shibuyaku,
Tokyo 150-0043

P +81 3 4360 5473
F +81 3 4360 5301
W bsa.org

Japan Representative Office

example, AI systems may unlawfully discriminate against individuals. As such, the public should be assured that such systems have been thoroughly vetted to identify and mitigate risks associated with unintended bias. In this respect, we support the White Paper's recommendations to build public confidence in AI by promoting the benefits of AI while encouraging reassessing safeguards for high-risk AI.

To achieve this objective, we provide the following recommendations and attach relevant documents which we hope will be useful in implementing the White Paper's recommendations. These include "Confronting Bias: A Framework to Build Trust in AI (BSA Framework)", a first-of-its-kind risk identification and mitigation impact assessment framework for AI systems,[4] and "AI Developers and Deployers: An Important Distinction", which explains the different roles of developers and deployers upon considering tailored obligations to an organization's role in the AI marketplace.[5]

We agree with the Project Team that AI products and services should be successfully adopted by building public trust and confidence in these technologies. To earn that trust, BSA encourages organizations that develop and use AI to account for the unique opportunities and risks the use of the technology poses. Policymakers can also enhance public confidence and trust in AI by establishing a legal and regulatory environment that supports responsible innovation.

As such, BSA recommends that any AI-related regulation should:

- apply only to high-risk AI systems;
- avoid prescriptive conformity assessment requirements;
- endorse the use of impact assessments;
- recognize the different roles and responsibilities of AI developers and deployers;
- align with emerging internationally recognized standards;
- incorporate a lifecycle approach to address responsible development and deployment of AI; and
- maintain data and intellectual property policies that promote innovation.

Regulations Should Apply Only to High-Risk AI Systems

The White Paper identifies three areas of risk to focus on for a new approach to AI regulation: 1) significant violations of human rights, 2) threats to national security, and 3) interference with democratic processes. We support the approach to limit the scope of potential regulations to high-risk uses. The AI ecosystem is broad, encompassing a diverse range of technologies and use cases and a wide array of stakeholders. Because the risks of AI are inherently use-case specific, any regulations should focus on specific applications of the technology that pose high risk to the public[6] and should be flexible enough to account for the unique considerations that may be implicated by specific use cases. It is important to define high risk use-cases and avoid a sectoral approach for determining risk. For example, payroll

[4] https://www.bsa.org/reports/confronting-bias-bsas-framework-to-build-trust-in-ai

[5] https://www.bsa.org/policy-filings/ai-developers-and-deployers-an-important-distinction

[6] High risk includes AI use cases involving a consequential decision, a determination made by a deployer that has a legal or similarly significant effect on an individual, for example, determination of an individual's eligibility for and results in the provision or denial of housing, employment, credit, education, access to physical places of public accommodation, healthcare, or insurance.

management AI or an AI system that is used for drafting documents (for example supporting word processing software with suggestions on synonyms or syntax), is not inherently high-risk, even if used in the context of national security.

We also encourage the Project Team to acknowledge the importance of maximizing AI use to mitigate the three risks identified in the white paper (i.e., significant violations of human rights, threats to national security, and interference with democratic processes), before regulating AI to address these risks. For example, AI technologies can provide solutions by detecting deep fakes or cyber-attacks, enhance cybersecurity, privacy, and child protection.[7]

Avoid Prescriptive Conformity Assessment Requirements

As highlighted above, the risks that AI poses and the appropriate mechanisms for mitigating those risks are largely context-specific. The appropriate mechanisms for the collection and use of training data, record keeping, transparency, accuracy, and human oversight will also vary depending on the nature of the AI system and the setting in which it is deployed. A prescriptive approach could impede efforts to address the very risks policy makers and governments intend to prevent, add unnecessary costs, and require extremely complex compliance checks. Regulation should focus instead on the factors stakeholders should consider in evaluating which metrics are relevant or appropriate for their use case. Regulators should avoid inflexible approaches and instead focus on process-based and outcome-oriented policy solutions that facilitate risk-based assessments. They should avoid establishing any pre-market conformity assessment for AI systems, as such obligations could act as unjustified market-entry barriers. Rather, a governance-based and self-attestation approach which identifies broad objectives and processes that developers and deployers should follow to achieve fairness in AI systems will be more effective. To this end, many global AI developers and deployers have taken voluntary steps to establish AI ethics principles and a formal review process built into companies' structure to help ensure that AI technologies are built and used safely and responsibly. The BSA Framework is an example of how industry stakeholders can come together to create a methodology for identifying and addressing AI risks.

Endorse the Use of Impact Assessments

We encourage AI regulation to endorse the use of impact assessments. One crucial safeguard that promotes responsible uses of AI is ensuring that companies that develop or use high-risk AI systems establish a comprehensive approach for performing impact assessments and design evaluations. Impact assessments are widely used in a range of other fields — from environmental protection to personal data protection — as an accountability mechanism that promotes trust by demonstrating that a system has been designed in a manner that accounts for the potential risks it may pose.

[7]For example, a cybersecurity company can use AI to assign a risk score to a login attempt which is based on information, such as the location of an IP address, which can then determine whether a malicious actor is attempting to log into another user's bank account and thus deny the login attempt. Also, by using machine learning and pattern matching, sensitive data hosted on cloud infrastructure can be discovered, enhancing privacy protection. Similarly, machine-learning models can be used for detecting manipulated media including deep fakes. AI tools can also be used to support law enforcement in combating child sexual abuse and exploitation online. These types of use cases illustrate the benefits that AI can bring and further demonstrate the need to consider the variety of positive applications in which AI can be used to protect individuals.

BSA supports requiring companies to conduct impact assessments and design evaluations for AI systems used to make consequential decisions. These assessments and evaluations are important accountability tools that help businesses identify, document, and mitigate AI risks. Notably, they are also helpful in detecting and mitigating potential biases that could result in unlawful discrimination. Any legislation requiring impact assessments and design evaluations should apply to high-risk uses and clearly distinguish requirements for developers and deployers.

Recognize the Different Roles and Responsibilities of AI Developers and Deployers

There are two key sets of actors that may bear varying degrees of responsibility for certain aspects of AI risk management:

- Developers: AI developers are organizations that design, code, or produce AI systems.

- Deployers: AI deployers are the organizations that adopt and use AI systems. (If an entity develops an AI system for its own use, it may be both the AI developer and the AI deployer.)

Policies and regulations should recognize this distinction and provide companies the flexibility to allocate risk contractually. Effective management of risks among these different actors will depend on the nature of the AI system being developed. Distinguishing between developers and deployers ensures that specified obligations reflect a company's role in the AI ecosystem. Tailoring obligations to a company's role as a developer or a deployer enables the company to fulfill the corresponding obligations and better protect consumers. For example, a developer is able to identify the source and describe the features of data used to train an AI system, but a developer generally would not have insight into how the AI system is used after another company has purchased and deployed the AI system. Instead, the deployer using the AI system is generally best positioned to understand how the system is being used, the outputs from the AI system, the nature of any customer complaints, and other real-world factors affecting the system's performance. Deployers are best positioned to understand the risk profile that an AI system may present to individuals. Ensuring AI policies create obligations that reflect these different roles will enable all stakeholders to better understand how their organizations can identify and address harmful bias in AI systems.

Align with Emerging Internationally Recognized Standards

As the Project Team and the Government explore new approaches to AI regulation, it is important to ensure that these are aligned with the emerging body of internationally recognized standards. This alignment will improve international interoperability and promote the ability of organizations in Japan, both AI developers and deployers, to benefit from the most advanced resource, concepts, and options available. The International Organization of Standardization's (**ISO**) Standards Committee on AI[8] has completed work on 10 sets of standards, including on bias in AI systems and approaches to enhance trustworthiness in AI.[9] The ISO Committee is currently developing 27 additional standards. The risk of establishing

[8] See ISO/IEC JTC 1/SC 42 at https://www.iso.org/committee/6794475.html

[9] See ISO/IEC TR 24027: 2021 (Bias in AI systems and AI aided decision making) at https://www.iso.org/standard/77607.html?browse=tc and ISO/IEC TR 24028:2020 (Overview of trustworthiness in artificial intelligence) at https://www.iso.org/standard/77608.html?browse=tc

domestic standards that are not well aligned with, or are too far ahead of, internationally recognized standards, is that requirements will be out of step with emerging practices, deterring development of AI in Japan and impeding efforts to ensure that the technology is developed and deployed responsibly.

Also, given that AI systems are developed and deployed in an international context, regulations and standards that apply to AI should operate across different jurisdictions to facilitate and promote further adoption and use of AI technologies. In this regard, we propose that Japan adopts the OECD's definition of AI. In its Recommendation of the Council on Artificial Intelligence (**Recommendation**),[10] the OECD defines AI as "a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations, or decisions influencing real or virtual environments", and specifies that AI systems are "designed to operate with varying levels of autonomy". This definition has been referenced by regulators worldwide, including the European Union.[11] The US National Institute of Standards and Technology (**NIST**) also adapts the OECD definition for use in its AI Risk Management Framework published in January.[12] Using an accepted and internationally recognized definition, such as the OECD's, will facilitate international alignment, dialogue, adoption, and compliance.

We also want to note efforts undertaken by industry bodies to voluntarily reduce the misuse of AI and other tools. For example, a multi-stakeholder community, the Content Authenticity Initiative (CAI),[13] promotes the adoption of an open industry standard for content authenticity and provenance. This enables viewers to know of the origins of the image or video, such as the photographer, the location where the image was generated, and if it was edited using software. This information assists viewers to determine the content's authenticity. The group, which has over 900 members, is currently developing open-source tools to help prevent misinformation and increase transparency around the use of AI. We encourage policymakers and the Government to support such efforts.

Incorporate a Lifecycle Approach to Address Responsible Development and Deployment of AI

Static evaluations of AI models cannot account for all potential issues that may arise when AI systems are deployed in the field. For example, bias can arise in a system at multiple points of its lifecycle and through many different channels. These include in the data used to train a model, in the formulation of the problem the system seeks to solve, or if a model is used in a scenario other than its intended purpose. AI risk management therefore requires a lifecycle approach that includes ongoing monitoring by end-users to ensure that the system is operating as intended. To address this issue, we encourage the Project Team and the

[10] Recommendation of the Council on Artificial Intelligence, May 2019, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449. Per the Recommendation, the AI stakeholder community "encompasses all organizations and individuals involved in, or affected by, AI systems, directly or indirectly."

[11] The European Union's draft Artificial Intelligence Act currently defines "artificial intelligence system" as "software that … can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with".

[12] NIST AI Risk Management Framework, January 26, 2023 at https://www.nist.gov/itl/ai-risk-management-framework

[13] See https://contentauthenticity.org/

Government to refer to the BSA Framework which identifies steps that can be taken in the design, development, and deployment stages of the AI lifecycle to mitigate the risk of bias.

Maintain Data and Intellectual Property Policies That Promote Innovation

The exponential increase in production of data, combined with increases in remote computing power and the development of more sophisticated algorithms, has fueled progress in AI. Capitalizing on these developments to facilitate continued advances in AI requires a sound data policy environment. International data transfers are integral to every stage of the AI lifecycle, from the development of predictive models to the deployment and use of AI systems. The data used in AI systems often originates from many geographically dispersed sources, making it imperative that data may be transferred across borders. Rules that unnecessarily limit cross-border data transfers invariably limit the benefits that AI systems can provide. Japan has acknowledged the importance of updating polices to foster innovation, proposing the concept of Data Free Flow with Trust (DFFT) to enable seamless and safe movement of data across borders[14]

We commend Japan's leadership in the recent G7 Digital and Tech Ministers' Meeting, encouraging G7 Parties to develop a harmonized, international framework for data transfers and AI utilization. Specifically, we are encouraged that the Ministerial Declaration[15] endorsed the establishment of the Institutional Arrangement for Partnership (IAP) to operationalize DFFT. We also welcome the adoption of the G7 Action Plan on AI[16], which promotes global interoperability between tools for trustworthy AI and AI governance frameworks around the world to enable an environment for AI innovation globally. We are eager to support these efforts. We also urge Japan to ensure that any new policy approaches on AI harmonize with positions taken by like-minded countries, such as US, EU, and other G7 countries.

In addition, in order to improve knowledge-sharing, collaboration, and development of new technologies like machine learning, Japan, along with the EU, has modernized its copyright law by adopting exceptions for text and data mining. This allows AI developers with lawful access to underlying works to use publicly available content to train AI systems, unlocking data insights that can be used for a myriad of valuable purposes. These are examples of policies that support investment and innovation and enable the benefits of AI for all.

Conclusion

BSA and our members look forward to working with the Project Team to support its goal of developing effective AI policies. In addition to sharing this recommendation, we would appreciate having continued opportunities for dialogues to better understand the White Paper's intention and discuss how we can further assist in the effort.

[14] See Data Free Flow with Trust (DFFT): Paths toward Free and Trusted Data Flows at https://jp.weforum.org/whitepapers/data-free-flow-with-trust-dfft-paths-towards-free-and-trusted-data-flows
[15] https://g7digital-tech-2023.go.jp/topics/pdf/pdf_20230430/ministerial_declaration_dtmm.pdf
[16] https://g7digital-tech-2023.go.jp/topics/pdf/pdf_20230430/annex5.pdf