Africa Tech For Development Initiative

25TH APRIL 2025

AFRICA TECH FOR DEVELOPMENT INITIATIVE(AFRICA4DEV) INPUT ON CALL FOR THE DEVELOPMENT OF ARTIFICIAL INTELLIGENCE (AI) ACTION PLAN FOR THE U.S BY THE NATIONAL SCIENCE FOUNDATION ON BEHALF OF THE OFFICE OF SCIENCE AND TECHNOLOGY POLICY (OSTP), THE NITRD NCO

1. INTRODUCTION

Artificial Intelligence (AI) is having tremendous impact on industries, economies, and societies globally and as AI technologies continue to evolve, their impact on governance, security, workforce development, and ethical considerations becomes increasingly significant. To maintain a competitive edge in AI development and deployment, the United States must adopt a comprehensive, forward-thinking AI Action Plan that prioritizes innovation, responsible governance, and strategic international collaboration.

Africa Tech for Development Initiative (Africa4Dev) is a leading organization committed to fostering responsible AI development, ethical AI policy, and inclusive technological advancement. Our mission is to ensure that AI benefits all communities, particularly in the Global South, by advocating for inclusive data representation, ethical AI standards, and sustainable AI policies. Africa4Dev believes that AI should not only serve technological and economic interests but also advance human rights, social good and equitable global participation in the AI-driven future.

A well-structured AI Action Plan will not only solidify the United States position as a global leader in AI but also ensure that its AI development aligns with democratic values, human rights, and international best practices. This proposed action plan presents the U.S. with a

towering opportunity to set down a landmark standard in AI governance one that is pro-innovation while simultaneously safeguarding fundamental rights and mitigating possible AI risks. It is extremely crucial to adopt resilient AI policies that foster transparency, accountability, and fairness more so as AI systems increasingly become vital in critical sectors such as finance, national security healthcare, and public services.

More so, AI is inherently global, requiring cross-border cooperation on regulatory frameworks, data-sharing mechanisms, and ethical AI development. Africa4Dev emphasizes the need for inclusive AI policymaking that considers diverse cultural, linguistic, and socio-economic perspectives. By fostering international collaboration especially with regions like Africa, where AI is emerging as a key driver of economic growth and digital transformation the U.S. can enhance its leadership role and contribute to building a globally inclusive AI ecosystem.

Through this submission, Africa4Dev aims to provide strategic insights and policy recommendations to help shape the U.S. AI Action Plan. Our recommendations address key policy areas, including cyber threats and data privacy, AI infrastructure, national security, trustworthiness, regulation, open-source development, explain ability, technical safety standards as well as research and development. We believe that an inclusive, well-regulated, and ethically governed AI ecosystem is not only essential for the U.S. but also for global AI development.

In this submission of input, we present concrete policy actions that will support AI innovation while ensuring responsible development, security, and sustainability. Integrating these policy measures will advance an exemplary U.S. leadership in AI development and regulation globally while also ensuring a robust AI future both for its heterogeneous and homogeneous population as well as the international community.

2. KEY AI POLICY AREAS AND CONCRETE POLICY ACTIONS

A. ADVANCEMENT IN HARDWARE AND CHIPS

Facts

Taiwan accounts for around 65% of global semiconductor supply, nearly 90% of the smallest and most sophisticated chips and Taiwan Semiconductor Manufacturing Co. (TSMC) is alone responsible for 55% of the world's supply[1]. As the dynamic advancement in the field of AI is heavily reliant on high-performance computing hardware, particularly semiconductors and AI-

[1] Robert J. Bowman, 'Supply Chain Brain, Does the U.S Need to Reduce its Dependence on Taiwan for Semiconductors?' https://www.supplychainbrain.com/blogs/1-think-tank/post/36085 accessed 3rd March 2025

optimized chips, the U.S. has historically led in semiconductor design, however global supply chain disruptions, geopolitical tensions, and increasing market competition from nations like China pose significant risks to AI hardware availability and innovation. The U.S. must implement robust policies that support semiconductor research, domestic manufacturing, and technological innovation in AI-specific hardware to maintain its leadership in AI development.

Recommendation

i. There should be stronger public-private partnerships between the U.S. government, leading chip manufacturers and research institutions to drive advancements in AI-optimized chip design.

ii. The US should endeavor to expand funding under the CHIPS and Science Act (2022) to specifically prioritize AI-driven hardware R&D, ensuring that AI applications are not bottlenecked by hardware limitations.

iii. AI chip design collaborations between academia and the private sector through post research grants, and shared R&D infrastructure to accelerate AI semiconductor innovation[2]. This will lead to innovations that will cut down on the high cost of building these chips.

iv. The US can accelerate domestic fabrication capacity for AI chips and such can be expanded through investments in U.S.-based semiconductor companies such as Micron which as $40 billion dollar plan to build memory manufacturing in the U.S, extension of partnership between Global foundries and Qualcomm, reducing reliance on Taiwan Semiconductor Manufacturing Company (TSMC) and South Korean firms.

v. The US need to implement a long-term AI Hardware Security and Supply Chain Resilience Strategy in collaboration with the Defense Advanced Research Projects Agency (DARPA) to ensure that AI chip production is safeguarded against geopolitical risks such as market forces and economic tensions and sanctions.

vi. Establish strategic reserves of critical raw materials (rare earth elements) needed for AI chip production to help forestall any unforeseen disruption in supply chain. Where this raw materials are not readily available in the US the US can strike a partnership deal with countries with huge quantity of such minerals making them shareholders in the AI ecosystem as this will guarantee long term access to this raw materials making it a win –win for both countries.

[2] CHIPS and Science Act of 2022, 'National Institute of Standards and Technology (NIST) Semiconductor Research Programs' (2022), https://www.nist.gov/news-events/news/2022/08/chips-and-science-act-2022-key-investments-us-innovation/ accessed 3rd March 2025

B. REDUCTION IN ENERGY CONSUMPTION BY DATA CENTERS

Facts

The demand for large-scale data centers continues to increase as artificial intelligence (AI) models become increasingly complex. While these data centers are essential for AI model training, storage, and processing, they consume vast amounts of energy and contribute significantly to carbon emissions. According to the International Energy Agency (IEA), data centers currently account for nearly 1% of global electricity consumption, with projections indicating continued increases as AI adoption expands[3].

The U.S must show commitment in the drive for environmental protection globally and should prioritize its leadership in the establishment of energy-efficient infrastructure and implement greener technologies incentives as this will ensure that AI development is sustainable and environmentally friendly. This AI policy must address the ease of scaling AI solutions while at same time ensuring they are environmentally sustainable so that AI-driven innovation does not come at the cost of environmental depletion. This is desirable because the world is currently grappling with challenges of high energy consumption by data centers and presents an opportunity for innovation leadership on the part of the U.S to halt this.

Recommendation

i. The US must push for federal agencies and government-funded AI research projects to use energy-friendly AI models that prioritize low-power AI hardware and optimized training algorithms as well as grants for AI data centers that utilize renewable energy sources.
ii. Encourage public-private partnerships between AI technology firms and energy companies to fund joint research on AI-driven clean energy solutions for data centers.
iii. Mandate research programs through government funding to enable innovations on smart grid technologies and machine learning models that optimize energy consumption in real time with the capacity to predict peak usage hours, adjust cooling systems dynamically, and optimize computational loads to reduce energy consumption.

[3] Thomas Spencer, Siddharth Singh, 'What the data centre and AI boom could mean for the energy sector' (October 18, 2024), https://www.iea.org/commentaries/what-the-data-centre-and-ai-boom-could-mean-for-the-energy-sector/ accessed 6th March 2025

C. OPEN-SOURCE AI MODEL DEVELOPMENT

Facts

Although Artificial Intelligence (AI) model development is becoming the fountain of innovation, driving advancements in healthcare, finance, education, and governance. However, as AI models become more powerful, concerns regarding transparency, accountability, and equitable access have emerged. The U.S. must implement policies that balance innovation, security, and ethical considerations, ensuring AI development benefits all sectors of society while maintaining its global leadership.

A huge challenge in AI governance is the level of non-transparency in foundational AI model and large-scale AI systems developed by private entities with minimal external oversight. These models, such as GPT-4, Gemini, Claude and Grok influence public discourse, decision-making, and critical infrastructure, yet their internal workings remain highly unknown. To ensure a secure and responsible AI ecosystem, U.S. policy must establish clear transparency standards and promote responsible open-source development amongst AI companies that develop AI-models.

Recommendation

i. Spread government grants for global open-source AI projects focused on ethical AI, security, and bias mitigation, ensuring that open AI models benefit education, research, and public-sector applications.

ii. Encourage partnerships between leading AI firms, universities, and research institutions globally to co-develop secure, high-quality open-source AI tools that align with U.S. strategic interests.

iii. Establish Transparency Requirements for Foundational AI Models to Promote Accountability in governance, data, performance, and monitoring to help federal agencies and others use AI responsibly as in line with the US Accountability office Accountability framework for Federal Agencies and other Entities[4]. The U.S can through its foreign relations department collaborate with other countries to adopt such transparency requirements.

iv. Exert explainability standards which will require AI companies to disclose model architectures, training datasets, and decision-making processes for high-risk AI applications, particularly in finance, healthcare, law enforcement, and national security.

[4] GAO-21-519SP, 'Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities' (June 30, 2021), https://www.gao.gov/products/gao-21-519sp accessed 6th March 2025

v. Establish an AI Model Oversight Body under the National Institute of Standards and Technology (NIST) or the Federal Trade Commission (FTC) to conduct independent audits of AI models, ensuring they comply with ethical and legal requirements.

vi. Require AI developers to submit bias impact assessments before deploying AI models at scale. This aligns with initiatives such as the EU AI Act's risk-based approach to AI regulation. Also there is need to develop a public AI transparency index to track how well AI models comply with transparency and accountability requirements. This will drive transparency as well as guarantee adherence to ethical standards.

D. USE OF AI APPLICATIONS IN THE PRIVATE SECTOR AND GOVERNMENT

Facts

Artificial Intelligence (AI) has had transformative impact is in several industries, while driving efficiency, innovation, and economic growth across the private and public sectors. AI adoption in government operations can streamline public services, defense strategies, and regulatory compliance. A good example is the launch of new digital services to streamline military management by the Ukrainian Military[5]. Diia which is an exceptional digital service supports digitalization in Ukraine by strengthening the Government's capacity to deliver high quality and accessible digital services[6].

The unregulated expansion of AI poses risks, including bias in decision-making, job displacement, cyber security threats, and ethical concerns. To ensure trustworthy AI deployment, U.S. policy must establish impact assessment frameworks, ethical guidelines, and human oversight mechanisms, safeguarding fairness, accountability, and national security while maintaining a competitive edge.

Recommendation

i. AI tools used in critical medical operations and decision-making should be subjected to FDA approval and periodic algorithmic audits to ensure accuracy and patient safety as well as require explainability from decisions of AI systems.

ii. Organizations deploying AI in high-risk sectors should be required to conduct AI Impact Assessments (AIAs) before public deployment.

iii. There should be expansion on AI adoption in social services, public safety, transportation, and defense to improve operational efficiency and citizen engagement.

---

[5] EGA, 'The Ukrainian defence sector launched new digital services'(November 15, 2024), https://ega.ee/ukrainian-defence-sector-launched-new-digital-services/ accessed 6th March 2025

[6] UNDP, 'Digital Inclusive, Accessible: Support to Digitalization of Public Services in Ukraine Project (DIA Support Project)', https://www.undp.org/ukraine/projects/digital-inclusive-accessible-support-digitalisation-public-services-ukraine-dia-support-project accessed 6th March 2025

In achieving this, the success road map of the Ukrainian Government should be understudied.

iv. A human interface framework to review AI driven recommendations used in critical public sectors should be implemented.

E. ASSURANCE AND EXPLAINABILITY OF AI MODEL OUTPUTS

Facts

As global AI regulations gains prominence, there is now an increasing need for explainability and interpretation with more organizations seeking guidelines on how to determine what level of explainability to adopt and how much information to release about their models. The EU Act[7], for example, imposes specific transparency requirements for different AI use cases classified according to its risk-based framework.

Recommendation

It is crucial that the U.S Government tasks AI Actors to 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 in order to achieve the following:

a. Foster a general understanding of AI systems, including their capabilities and limitations.
b. Make stakeholders aware of their interactions with AI systems, including in the workplace.
c. Where feasible and useful, to provide plain and easy-to-understand information on the sources of data/input, factors, processes and/or logic that led to the prediction, content, recommendation or decision, to enable those affected by an AI system to understand the output.
d. Provide information that enables those adversely affected by an AI system to challenge its output[8].

Organizations should be tasked on developing on roadmap for Explainability and Assurance of AI Model Outputs through building the right XAI team, establishing the right mindset,

[7] The EU Artificial Intelligence Act, 'Up-to-date developments and analyses of the EU AI Act', https://artificialintelligenceact.eu/ accessed 7th March 2025

[8] OECD, 'OECD Transparency and explainability (Principle 1.3)', https://oecd.ai/en/dashboards/ai-principles/P7 accessed 12th March 2025

defining clear objectives, developing an action plan, measuring metrics and benchmarks, selecting or building appropriate tools, monitor and iterate[9].

F. CYBERSECURITY, DATA PRIVACY, AND AI MODEL SECURITY

Facts

The integration of AI systems into healthcare, finance, public service and even defense opens up the possibility for vulnerability to cyber-attacks, third party manipulation and data breaches. More so as AI in increasing gaining traction for use by individuals, privacy concerns continue to emerge as large-scale datasets containing sensitive information of users are used to train models often times without their consent. Thus without efficient cyber security measures, regulatory oversight, and ethical AI frameworks, these risks could undermine public trust, economic stability, and national security.

Existing privacy frameworks have gaps in protecting individuals in an AI-driven world. For example, there are challenges in proving that fundamental rights have been violated and/or harm produced in a digital context. However, views among stakeholders continue to differ on the role of regulation in protecting privacy. While some prefer more regulation, others advocate for a heavier reliance on business codes of conduct, technical tools, contract terms, and other devices that are not legally binding. This often is referred to as a "soft law" approach. Data scraping for generative AI and other purposes has led to numerous enforcement and litigation across jurisdictions, raising privacy, intellectual property litigation across jurisdictions, raising privacy, intellectual property and other concerns[10].

About 40% of IT professionals in the U.S believe that cyber security and privacy concerns are the main challenges related to AI[11]. Similarly, in 2024 about 39% of small companies experienced both security and data breaches in the U.S[12]. To maintain the integrity, security, and fairness of AI systems, the U.S. must develop robust policies that address AI-specific

---

[9] Carlo Giovine, Roger Roberts with Mara Pometti and Medha Bankhwal 'Building AI trust: The key role of explainability' (November 26, 2024) https://www.mckinsey.com/capabilities/quantumblack/our-insights/building-ai-trust-the-key-role-of-explainability accessed 12th March 2025

[10] ArentFox Schiff, 'litigation across jurisdictions, raising privacy, intellectual property and other concerns' (July 18, 2023), https://www.jdsupra.com/legalnews/data-scraping-privacy-law-and-the-3354981/ accessed 12th March 2025

[11] Alexandra Borgeaud, 'Main challenges expected or experienced due to artificial intelligence (AI) in the United States in 2024'(Statista February 25, 2025), https://www.statista.com/statistics/1550573/us-top-ai-challenges-for-companies-worldwide/ accessed 12th March 2025

[12] Statista, 'Types of cyber incidents experienced by small companies in the United States as of August 2024' (March 11, 2025), https://www.statista.com/statistics/1455155/types-of-cyber-attacks-companies-in-the-us/ accessed 12th March 2025

cyber security challenges, adversarial risks, and data privacy concerns while aligning with global best practices in AI governance.

Recommendation

The U.S should adopt the Key pillars to protect privacy and other fundamental rights in an AI-driven world[13].

i. Inclusive dialogue

Since privacy and other fundamental rights impact everyone, the process for developing safeguards must involve the global community and diverse stakeholders, such as historically under-represented groups in the U.S. The dialogue should also include experts from multiple disciplines to help ensure that technical and other profiles can widely operationalize legal and policy approaches in a compliant, ethical, and sustainable manner.

ii. Common definitions

Even within the privacy and AI realms, a single term can have different meanings. Technical and non-technical experts often have different lexicons. The U.S should adopt common definitions on an international level and across sectors as this would help support inclusive dialogue on AI by bridging differences among jurisdictions and facilitating multi-disciplinary communications and collaborations. More progress in creating uniform definitions will bolster common understandings and advance the U.S leadership.

iii. Addressing data scraping

In Europe the EDPS was launched a task force on ChatGPT[14]. The EDPB adopted a dispute resolution decision on the basis of Art. 65 GDPR concerning a draft decision of the IE DPA on the legality of data transfers to the United States by Meta Platforms Ireland Limited (Meta IE) for its Facebook service. The U.S government must adopt similar measures to continue to address data scraping and keep AI companies in check against data privacy breaches.

iv. Strengthen AI-specific Cyber security Protocols to protect against adversarial attacks by setting up a National AI security Unit that will mandated to conduct regular AI security audits and stress tests to identify vulnerabilities in government and private-sector AI applications as well as respond to AI threats, detect ad provide defense mechanisms.

[13] Lee Tiedrich, Celine Caira, Yaniv Benhamou, 'The AI data challenge: How do we protect privacy and other fundamental rights in an AI-driven world?' (October 19, 2023), https://oecd.ai/en/wonk/the-ai-data-challenge-how-do-we-protect-privacy-and-other-fundamental-rights-in-an-ai-driven-world?trk=public_post_comment-text accessd 12th March 2025

[14] European Data Protection Board, 'EDPB resolves dispute on transfers by Meta and creates task force on Chat GPT' (April 13, 2023), https://www.edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en accessed 12th March 2025

v. Enhance Supply Chain Security for AI Models and Hardware through implementation of strict security requirements for AI supply chains, including chip manufacturing, cloud computing services, and open-source AI tools while also mandating federal AI vendors to comply with zero-trust security architectures and encryption standards[15].

vi. Develop National AI data privacy laws that align with global best Practices. The U.S should enact a federal AI data privacy law similar to the European Union's General Data Protection Regulation (GDPR) as well as issue compelling clear guidelines for AI data collection, processing, and retention; ensuring users have full control over their personal data at every stage of the data lifecycle.

vii. Advance legislations in localizing sensitive data to be used exclusively within the U.S while non-sensitive data can be shared under a responsible and ethical data utility Agreement to be entered into by regional countries. This will help advance global AI development and halt underrepresentation in datasets and algorithmic bias.

G. RESEARCH AND DEVELOPMENT (R&D)

Facts

Greater investments in artificial intelligence research and development are essential to maintaining American leadership in AI. Throughout the 20th century, the federal government played a critical role in fueling technological innovation by funding pivotal basic research. Government funding was essential to developing the transistor, GPS, and the internet inventions that transformed the world economy. Yet over the past several decades, federal government spending on R&D as a percentage of GDP declined from about 1.2% in 1976 to around 0.7% in 2018[16]. This is a worrisome trend as the federal government remains the main funder of basic research. Government support again could be pivotal both in fostering new AI breakthroughs and ensuring that the U.S. government has access to those breakthroughs. Beyond AI, overall R&D spending trends are troubling. Other countries are outpacing the United States with faster growth of their national R&D budgets. Total U.S. national (public and private) R&D expenditures as a share of GDP have been mostly stagnant since 1996. China quadrupled its R&D expenses as a share of GDP over the same time frame, and countries like Israel and South Korea also significantly ramped up spending[17].

---

[15] NIST, 'AI Risk Management Framework' (January 5, 2025), https://www.nist.gov/itl/ai-risk-management-framework accessed 12th March 2025

[16] AAAS, 'Federal R&D as a Percent of GDP' (June 2019), https://www.aaas.org/sites/default/files/2019-06/RDGDP.png accessed 12th March 2025

[17] World Bank, 'Research and development expenditure (percent of GDP), 1996-2017' (The World Bank, 2017), https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS. accessed 12th March 2025

The U.S. government remains the largest funder of basic research in the United States[18]. As during the 1960s and 1970s, government support again could be pivotal today both in fostering new breakthroughs and ensuring that the U.S. government has access to them. The federal government should prioritize a high T risk/high-reward basic science research area where private industry has little incentive to invest but that holds tremendous potential for valuable new knowledge. Breakthroughs in software, such as novel AI techniques that address the limitation of existing AI methods, and hardware, such as next generation semiconductor technologies and superconducting artificial neurons, could be game changers that provide the United States with a continuing technological edge. Advances in AI can also further R&D of other fields because of its broad, interdisciplinary nature, while breakthroughs in areas like neuroscience can greatly advance AI development.

Recommendation

i. The National Science Foundation should work with science funding organizations in allied countries to establish multilateral teams of AI researchers from the public and private sectors to promote talent development and foster partnerships on AI R&D. Furthermore, like academia, the government cannot compete with the private sector in terms of salaries. However, like academia, it can provide workers with opportunities not seen in private R&D including making public policy, experimenting in novel fields that are unrelated to the need to commercialize a technology and the opportunity to serve the public good. Additionally, the federal government needs tech experts to effectively create, manage, and implement AI-related R&D grants. To bring more tech expertise into the federal government, employment processes should be addressed through the creation of fellowship programs, inefficiencies in the hiring process, and enable tech experts to float between agencies.

ii. There needs to be international cooperation to advance AI research and development as an open democratic society with world-class universities, research institutes, and corporations, the United States makes for an attractive partner in joint R&D.

iii. Overall AI R&D spending needs to increase significantly Support AI for Social Good Initiatives particularly incentives for startups and non-profits developing AI for public health, environmental sustainability, and accessibility as well as investments in explainable AI (XAI), fairness, and AI ethics to mitigate algorithmic bias and improve decision-making transparency.

[18] Bipartisan Policy Center, Cementing American Artificial Intelligence Leadership: AI Research & Development (August 2020) available at https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2020/08/BPC_RD-AI-Paper_RV5.pdf accessed 12th March 2025

iv. AI researchers should be required to collaborate with experts in human rights, philosophy, and regulatory policy to ensure responsible development. The U.S. Department of State released a Risk Management Profile for Artificial Intelligence and Human Rights[19] as a practical guide for organizations including governments, the private sector, and civil society to design, develop, deploy, use, and govern AI in a manner consistent with respect for international human rights[20].

v. Establish AI Ethics and Governance Research Centers in Universities. Funds dedicated to these centers should be tailored towards advancing research in AI policy, governance, and ethical AI development. Research conducted here should be interdisciplinary comprising of ethics, law, and social sciences and should delve into most crucial areas of AI's impact on areas such as privacy, labour markets, democracy, and misinformation.

CONCLUSION

Africa4Dev remains committed to championing responsible AI policy, ethical governance, and equitable technological advancements. As artificial intelligence continues to reshape economies, governance, and societal structures, it is imperative that AI policies prioritize inclusivity, transparency, and accountability. The U.S., as a global leader in AI development, must set a precedent for ethical AI deployment by ensuring that AI systems are safe, fair, and aligned with human rights principles. A comprehensive and forward-thinking AI Action Plan will not only solidify the U.S' leadership but also foster global trust, innovation, and cross-border collaboration.

Africa4Dev calls on governments, private sector leaders, researchers, and civil society to work together in shaping an AI ecosystem that benefits all, safeguards democratic values, and promotes sustainable development. By adopting inclusive AI strategies and prioritizing diverse data representation, we can collectively ensure that AI serves as a force for good empowering communities, driving economic growth, and enhancing global cooperation.

[19] U.S Department of State Bureau of Cyberspace and Digital Policy, 'Risk Management Profile for Artificial Intelligence and Human Rights' (July 25, 2024), https://2021-2025.state.gov/risk-management-profile-for-ai-and-human-rights/ accessed 13th March 2025

[20] NIST, 'AI Risk Management Framework, https://www.nist.gov/itl/ai-risk-management-framework accessed 13th March 2025

REFERENCES

AAAS, 'Federal R&D as a Percent of GDP' (June 2019), https://www.aaas.org/sites/default/files/2019-06/RDGDP.png accessed 12th March 2025

Alexandra Borgeaud, 'Main challenges expected or experienced due to artificial intelligence (AI) in the United States in 2024'(Statista February 25, 2025), https://www.statista.com/statistics/1550573/us-top-ai-challenges-for-companies-worldwide/ accessed 12th March 2025

ArentFox Schiff, 'litigation across jurisdictions, raising privacy, intellectual property and other concerns' (July 18, 2023), https://www.jdsupra.com/legalnews/data-scraping-privacy-law-and-the-3354981/ accessed 12th March 2025

Bipartisan Policy Center, Cementing American Artificial Intelligence Leadership: AI Research & Development (August 2020) available at https://bipartisanpolicy.org/download/?file=/wp-content/uploads/2020/08/BPC_RD-AI-Paper_RV5.pdf accessed 12th March 2025

Carlo Giovine, Roger Roberts with Mara Pometti and Medha Bankhwal 'Building AI trust: The key role of explainability' (November 26, 2024) https://www.mckinsey.com/capabilities/quantumblack/our-insights/building-ai-trust-the-key-role-of-explainability accessed 12th March 2025

CHIPS and Science Act of 2022, 'National Institute of Standards and Technology (NIST) Semiconductor Research Programs' (2022), https://www.nist.gov/news-events/news/2022/08/chips-and-science-act-2022-key-investments-us-innovation/ accessed 3rd March 2025

EGA, 'The Ukrainian defence sector launched new digital services'(November 15, 2024), https://ega.ee/ukrainian-defence-sector-launched-new-digital-services/ accessed 6th March 2025

European Data Protection Board, 'EDPB resolves dispute on transfers by Meta and creates task force on Chat GPT' (April 13, 2023), https://www.edpb.europa.eu/news/news/2023/edpb-resolves-dispute-transfers-meta-and-creates-task-force-chat-gpt_en accessed 12th March 2025

GAO-21-519SP, 'Artificial Intelligence: An Accountability Framework for Federal Agencies and Other Entities' (June 30, 2021), https://www.gao.gov/products/gao-21-519sp accessed 6th March 2025

Lee Tiedrich, Celine Caira, Yaniv Benhamou, 'The AI data challenge: How do we protect privacy and other fundamental rights in an AI-driven world?' (October 19, 2023), https://oecd.ai/en/wonk/the-ai-data-challenge-how-do-we-protect-privacy-and-other-fundamental-rights-in-an-ai-driven-world?trk=public_post_comment-text accessd 12th March 2025

NIST, 'AI Risk Management Framework' (January 5, 2025), https://www.nist.gov/itl/ai-risk-management-framework accessed 12th March 2025

OECD, 'OECD Transparency and explainability (Principle 1.3)', https://oecd.ai/en/dashboards/ai-principles/P7 accessed 12th March 2025

Robert J. Bowman, 'Supply Chain Brain, Does the U.S Need to Reduce its Dependence on Taiwan for Semiconductors?' https://www.supplychainbrain.com/blogs/1-think-tank/post/36085 accessed 3rd March 2025

Statista, 'Types of cyber incidents experienced by small companies in the United States as of August 2024' (March 11, 2025), https://www.statista.com/statistics/1455155/types-of-cyber-attacks-companies-in-the-us/ accessed 12th March 2025

The EU Artificial Intelligence Act, 'Up-to-date developments and analyses of the EU AI Act', https://artificialintelligenceact.eu/ accessed 7th March 2025

Thomas Spencer, Siddharth Singh, 'What the data centre and AI boom could mean for the energy sector' (October 18, 2024), https://www.iea.org/commentaries/what-the-data-centre-and-ai-boom-could-mean-for-the-energy-sector/ accessed 6th March 2025

UNDP, 'Digital Inclusive, Accessible: Support to Digitalization of Public Services in Ukraine Project (DIA Support Project)', https://www.undp.org/ukraine/projects/digital-inclusive-accessible-support-digitalisation-public-services-ukraine-dia-support-project accessed 6th March 2025

U.S Department of State Bureau of Cyberspace and Digital Policy, 'Risk Management Profile for Artificial Intelligence and Human Rights' (July 25, 2024), https://2021-2025.state.gov/risk-management-profile-for-ai-and-human-rights/ accessed 13th March 2025

World Bank, 'Research and development expenditure (percent of GDP), 1996-2017' (The World Bank, 2017), https://data.worldbank.org/indicator/GB.XPD.RSDV.GD.ZS. accessed 12th March 2025

Majiuzu Daniel Moses
Executive Director
Africa Tech for Development Initiative - Africa4dev
info@africa4dev.org; mmajiuzu@gmail.com
www.africa4dev.org
+2348063154897

"THIS DOCUMENT IS APPROVED FOR PUBLIC DISSEMINATION. THE DOCUMENT CONTAINS NO BUSINESS-PROPRIETARY OR CONFIDENTIAL INFORMATION. DOCUMENT CONTENTS MAY BE REUSED BY THE GOVERNMENT IN DEVELOPING THE AI ACTION PLAN AND ASSOCIATED DOCUMENTS WITHOUT ATTRIBUTION."