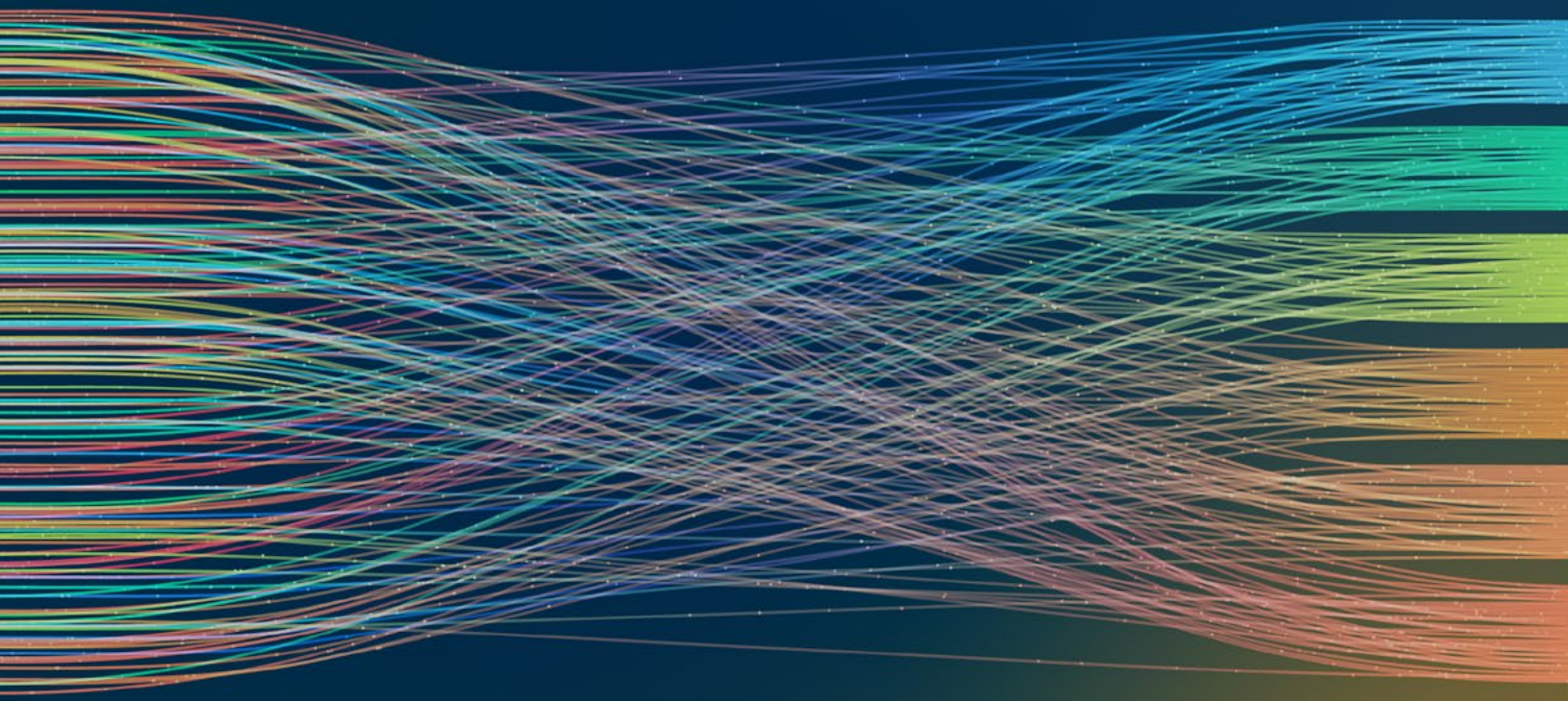
OCTOBER 2021

STRENGTHENING INTERNATIONAL COOPERATION ON AI

PROGRESS REPORT



CAMERON F. KERRY
JOSHUA P. MELTZER
ANDREA RENDA
ALEX C. ENGLER
ROSANNA FANNI

BROOKINGS

CEPS

STRENGTHENING INTERNATIONAL COOPERATION ON AI

PROGRESS REPORT

October 2021

CAMERON F. KERRY
JOSHUA P. MELTZER
ANDREA RENDA
ALEX C. ENGLER
ROSANNA FANNI

CONTENTS

PREFACE

Recognizing the strategic, economic, and social significance of artificial intelligence (AI), numerous governments have adopted strategies to meet the challenges and opportunities of this technology. Originally focused on industrial competitiveness and investment in research and innovation, policymakers are also assessing the risks of AI for fundamental rights and safety. The pursuit of responsible AI—AI that is ethical, trustworthy, and reliable—is increasingly central to many governments' AI policy, a focus for AI research and development, and a concern for civil society eager to maximize the opportunities of AI while mitigating its risks.

These issues transcend national boundaries. As a result, international cooperation on AI policy and development has become an important element of national policies and a focus for international bodies. In 2019, The Brookings Institution and the Centre for European Policy Studies (CEPS) saw a need for deeper exploration of international cooperation in AI development and policymaking and established the Forum for Cooperation on AI (FCAI), a high-level exchange among government officials and leading experts from academia, the private sector, and civil society. Beginning as a transatlantic dialogue among Canada, the EU, the U.K. and the U.S., FCAI expanded to encompass Australia, Japan, and Singapore, and convened eight roundtables among officials and experts over a 12-month period since June 2020. In addition to group discussions, the authors conducted numerous interviews with individual participants as well as research on developments in artificial intelligence and international AI policy.

The seven governments involved are global leaders in AI policy development and investment and are linked by trade, security interests, and common democratic values. Together, they represent almost 50 percent of global GDP and contain the majority of the world's research, talent, and commerce in AI. All have been involved in international discussions of cooperation.

This progress report outlines the preliminary findings and recommendations of the FCAI on ways to build on these discussions and enhance international cooperation toward responsible AI that harnesses the benefits and manages the risks for humanity. The report identifies concrete steps that would benefit international cooperation, as well as subjects that will be explored by FCAI in greater depth over the coming months.

ACKNOWLEDGMENTS

The authors thank Karim Abdelnour, Caitlin Chin, and Aaron Tielemans of The Brookings Institution and Moritz Laurer of CEPS for their assistance with research and project management; and David Batcheck of Brookings for design and production. In addition, they are grateful to John Allen and Chris Meserole of Brookings for their active engagement with this project. Rosanna Fanni gives thanks to the Fulbright-Schuman Program for funding a visiting researcher stay at Brookings in 2020-2021.

The Brookings Institution is a nonprofit organization devoted to independent research and policy solutions. Its mission is to conduct high-quality, independent research and, based on that research, to provide innovative, practical recommendations for policymakers and the public. The conclusions and recommendations of any Brookings publication are solely those of its authors, and do not reflect the views of the Institution, its management, or its other scholars.

Amazon, Apple, Department of State, Deloitte, Facebook, Google, IBM, McKinsey & Company, Microsoft, MasterCard, National Science Foundation, Salesforce, University of Pennsylvania, and the World Bank are donors to the Brookings Institution. Brookings and CEPS recognize that the value they provide is in its absolute commitment to quality, independence, and impact. The findings, interpretations, and conclusions in this report are not influenced by any donation.

The Centre for European Policy Studies (CEPS) is an independent policy research institute in Brussels. Its mission is to produce sound policy research leading to constructive solutions to the challenges facing Europe. Facebook, Google, and Microsoft are donor members of CEPS. The views expressed in this report are entirely those of the authors and should not be attributed to CEPS or any other institution with which they are associated or to the European Union.

AUTHORS

Cameron F. Kerry is the Ann R. and Andrew H. Tisch distinguished visiting fellow at The Brookings Institution. In addition to his work at Brookings, Kerry is also a visiting scholar with the MIT Media Lab. Previously, he served as General Counsel and Acting Secretary of the U.S. Department of Commerce, where he led the Obama administration's work on consumer privacy, including the Consumer Privacy Bill of Rights. He has also spent time in private practice as a litigator and regulatory lawyer.

Joshua P. Meltzer is a senior fellow at The Brookings Institution, where his research focuses on digital trade, emerging technologies, and AI. Meltzer has testified before the U.S. Congress, the U.S. International Trade Commission, and the European Parliament. He has been an expert witness in litigation on data flows and privacy issues in the EU and a consultant to the World Bank on trade and privacy matters. Meltzer is a member of Australia's National Data Advisory Council and a member of Australia's AI Action Plan Programs Committee. Meltzer teaches digital trade law at Melbourne University Law School and at the University of Toronto Law School, where he is an adjunct professor, and teaches ecommerce and digital trade at the UK Foreign, Commonwealth and Development Office diplomatic academy. Prior to joining Brookings, Meltzer was posted as a diplomat at the Australian Embassy in Washington D.C. and before that was a trade negotiator in Australia's Department of Foreign Affairs and Trade.

Andrea Renda is a senior research fellow and head of Global Governance, Regulation, Innovation and the Digital Economy (GRID) at CEPS. He is also a non-resident Senior Fellow at Duke University's Kenan Institute for Ethics, and was Adjunct Professor of Law and Economics at Duke Law School during the 2016-17 academic year. His current research interests include regulation and policy evaluation, regulatory governance, private regulation, innovation, internet, and competition policies, as well as the alignment of policies such as sustainability and decarbonization with long-term impacts.

Alex C. Engler is a fellow in Governance Studies at The Brookings Institution, where he studies the implications of artificial intelligence and emerging data technologies on society and governance. Engler also teaches classes on data science and visualization at Georgetown University's McCourt School of Public Policy, where he is an adjunct professor and affiliated scholar. In 2021, Engler was awarded a Fulbright-Schuman Innovation Award to study European AI and digital governance in Berlin and Brussels. Before Brookings, Mr. Engler was faculty at the University of Chicago, where he ran the M.S. in Computational Analysis and Public Policy. He also brings a decade of experience as a data scientist at policy institutions such as MDRC and the Urban Institute.

Rosanna Fanni is an associate research Assistant and digital forum coordinator within the Global Governance, Regulation, Innovation and the Digital Economy (GRID) unit at CEPS. Toward her work on norms, technology policy, and international relations, she was a 2020-2021 Fulbright-Schuman Grantee and Visiting Researcher at The Brookings Institution. She is also an incoming PhD Fellow at the GIGA Institute, where she will analyze transnational governance architectures and algorithmic infrastructures with a focus on the Global South.

ABBREVIATIONS

3GPP	3rd Generation Partnership Project
AI Act	The European Commission's proposed Regulation on a European Approach for Artifical Intelligence
AI HLEG	High-Level Expert Group for AI
AISG	AI Singapore
ALLEA	European Federation of Academies of Sciences and Humanities
APEC	Asia Pacific Economic Cooperation
AUSTRAC	Australian Transaction Reports and Analysis Centre
B2B	business-to-business
BEUC	European Consumer Organisation
BSI	British Standards Institution
CAHAI	Committee on Artificial Intelligence
CBPR	“Cross-Border Privacy Rules” – APEC
CEPS	Centre for European Policy Studies
CERN	Conseil Européen pour la Recherche Nucléaire, or European Center for Nuclear Research
CFPB	Consumer Financial Protection Bureau
CIFAR	Canadian Institute for Advanced Research
CLAIRE	Confederation of Laboratories for Artificial Intelligence in Europe
CoE	Council of Europe
CSIRO	Commonwealth Scientific and Industrial Research Organization
DFFT	Data Free Flow with Trust
EASAC	European Academies’ Science Advisory Council
EDRi	European Digital Rights
EO	U.S. executive order
FCAI	Forum for Cooperation on AI

FEAM	Federation of European Academies of Medicine
GDPR	EU General Data Protection Regulation
GPAI	Global Partnership on AI
GTFS	General Transit Feed Specification
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IRC	international regulatory cooperation
ISO	International Organization for Standardization
IT	information technology
ITU	International Telecommunication Union
METI	Japan's Ministry of Economy, Trade and Industry
ML	machine learning
NDAA	National Defense Authorization Act – USA
NSCAI	U.S. National Security Commission on Artificial Intelligence
OECD	Organization for Economic Cooperation and Development
OECD.AI	OECD.AI Policy Observatory
ONE AI	OECD Network of Experts on AI
PDPA	Personal Data Protection Act – Singapore
PIPEDA	Personal Information Protection and Electronic Documents Act
PPC	privacy preserving computation
R&D	research and development
SA	Standards Australia
SAC	Standards Administration of China
SCC	Standards Council of Canada
SDGs	U.N. Sustainable Development Goals
SDOs	standards development organizations
TBT	Technical Barriers to Trade
UN	United Nations
WEF	World Economic Forum
WTO	World Trade Organization

EXECUTIVE SUMMARY

International cooperation on artificial intelligence—why, what, and how

Since 2017, when Canada became the first country to adopt a national AI strategy, at least 60 countries have adopted some form of policy for artificial intelligence (AI). The prospect of an estimated boost of 16 percent, or US$13 trillion, to global output by 2030 has led to an unprecedented race to promote AI uptake across industry, consumer markets, and government services. Global corporate investment in AI has reportedly reached US$60 billion in 2020 and is projected to more than double by 2025.

At the same time, the work on developing global standards for AI has led to significant developments in various international bodies. These encompass both technical aspects of AI (in standards development organizations (SDOs) such as the International Organization for Standardization (ISO), the International Electrotechnical Commission (IEC), and the Institute of Electrical and Electronics Engineers (IEEE) among others) and the ethical and policy dimensions of responsible AI. In addition, in 2018 the G-7 agreed to establish the Global Partnership on AI, a multistakeholder initiative working on projects to explore regulatory issues and opportunities for AI development. The Organization for Economic Cooperation and Development (OECD) launched the AI Policy Observatory to support and inform AI policy development. Several other international organizations have become active in developing proposed frameworks for responsible AI development.

In addition, there has been a proliferation of declarations and frameworks from public and private organizations aimed at guiding the development of responsible AI. While many of these focus on general principles, the past two years have seen efforts to put principles into operation through fully-fledged policy frameworks. Canada's directive on the use of AI in government, Singapore's Model AI Governance Framework, Japan's Social Principles of Human-Centric AI, and the U.K. guidance on understanding AI ethics and safety have been frontrunners in this sense; they were followed by the U.S. guidance to federal agencies on regulation of AI and an executive order on how these agencies should use AI. Most recently, the EU proposal for adoption of regulation on AI has marked the first attempt to introduce a comprehensive legislative scheme governing AI.

Global corporate investment in AI has reportedly reached US$60 billion in 2020 and is projected to more than double by 2025.

In exploring how to align these various policymaking efforts, we focus on the most compelling reasons for stepping up international cooperation (the "why"); the issues and policy domains that appear most ready for enhanced collaboration (the "what"); and the instruments and forums that could be leveraged to achieve meaningful results in advancing international AI standards, regulatory cooperation, and joint R&D projects to tackle global challenges (the "how"). At the end of this report, we list the topics that we propose to explore in our forthcoming group discussions.

Even more than many domains of science and engineering in the 21st century, the international AI landscape is deeply collaborative, especially when it comes to research, innovation, and standardization.

Why international cooperation on AI is important

Even more than many domains of science and engineering in the 21st century, the international AI landscape is deeply collaborative, especially when it comes to research, innovation, and standardization. There are several reasons to sustain and enhance international cooperation.

1. **AI research and development is an increasingly complex and resource-intensive endeavor, in which scale is an important advantage.** Cooperation among governments and AI researchers and developers across national boundaries can maximize the advantage of scale and exploit comparative advantages for mutual benefit. An absence of international cooperation would lead to competitive and duplicative investments in AI capacity, creating unnecessary costs and leaving each government worse off in AI outcomes. Several essential inputs used in the development of AI, including access to high-quality data (especially for supervised machine learning) and large-scale computing capacity, knowledge, and talent, benefit from scale.

2. **International cooperation based on commonly agreed democratic principles for responsible AI can help focus on responsible AI development and build trust.** While much progress has been made aligning on responsible AI, there remain differences—even among Forum for Cooperation on AI (FCAI) participants. The next steps in AI governance involve translating AI principles into policy, regulatory frameworks, and standards. These will require deeper understanding of how AI works in practice and working through the operation of principles in specific contexts and in the face of inevitable tradeoffs, such as may arise when seeking AI that is both accurate and explainable. Effective cooperation will require concrete steps in specific areas, which the recommendations of this report aim to suggest.

3. **When it comes to regulation, divergent approaches can create barriers to innovation and diffusion.** Governments' efforts to boost domestic AI development around concepts of digital sovereignty can have negative spillovers, such as restrictions on access to data, data localization, discriminatory investment, and other requirements. Likewise, diverging risk classification regimes and regulatory requirements can increase costs for businesses seeking to serve the global

AI market. Varying governmental AI regulations may necessitate building variations of AI models that can increase the work necessary to build an AI system, leading to higher compliance costs that disproportionately affect smaller firms. Differing regulations may also force variation in how data sets are collected and stored, creating additional complexity in data systems and reducing the general downstream usefulness of the data for AI. Such additional costs may apply to AI as a service as well as hardware-software systems that embed AI solutions, such as autonomous vehicles, robots, or digital medical devices. Enhanced cooperation is key to create a larger market in which different countries can try to leverage their own competitive advantage. For example, the EU seeks to achieve a competitive advantage in "industrial AI:" EU enterprises could exploit that AI without the prospect of having to engage in substantial re-engineering to meet requirements of another jurisdiction.

4. **Aligning key aspects of AI regulation can enable specialized firms in AI development to thrive.** Such companies generate business by developing expertise in a specialized AI system, then licensing these to other companies as one part of a broader tool. As AI becomes more ubiquitous, complex stacks of specialized AI systems may emerge in many sectors. A more open global market would allow a company to take advantage of digital supply chains, using a single product with a natural language model built in Canada, a video analysis algorithm trained in Japan, and network analysis developed in France. Enabling global competition by such specialized firms will encourage healthier markets and more AI innovation.

5. **Enhanced cooperation in trade is essential to avoid unjustified restrictions to the flow of goods and data, which would substantially reduce the prospective benefits of AI diffusion.** While the strategic importance of data and sovereignty has in many countries given rise to legitimate industrial policy initiatives aimed at mapping and reducing dependencies on the rest of the world, protectionist measures can jeopardize global cooperation, impinge on global value chains, and negatively affect consumer choice, thereby reducing market size and overall incentives to invest in meaningful AI solutions.

6. **Enhanced cooperation is needed to tap the potential of AI solutions to address global challenges.** No country can "go it alone" in AI, especially when it comes to sharing data and applying AI to tackle global challenges like climate change or pandemic preparedness. The governments involved in the FCAI share interests in deploying AI for global social, humanitarian, and environmental benefit. For example, the EU is proposing to employ AI to support its Green Deal, and the G-7 and GPAI have called for harnessing AI for U.N. Sustainable Development Goals. Collaborative "moonshots" can pool resources to leverage the potential of AI and related technologies to address key global problems in domains such as health care, climate science, or agriculture at the same time as they provide a way to test approaches to responsible AI together.

7. **Cooperation among likeminded countries is important to reaffirm key principles of openness and protection of democracy, freedom of expression, and other human rights.** The risks associated with the unconstrained use of AI solutions by techno-authoritarian regimes—such as China's—expose citizens to potential violations of human rights and threaten to split cyberspace into incompatible technology stacks and fragment the global AI R&D process.

The fact that international cooperation is an element of most governments' AI strategies indicates that governments appreciate the connection between AI development and collaboration across borders. This report is about concrete ways to realize this connection.

At the same time, international cooperation should not be interpreted as complete global harmonization: countries legitimately differ in national strategic priorities, legal traditions, economic structures, demography, and geography. International collaboration can nonetheless create the level-playing field that would enable countries to engage in fruitful "co-opetition" in AI: agreeing on basic principles and when possible seeking joint outcomes, but also competing for the best solutions to be scaled up at the global level. Robust cooperation based on common principles and values is a foundation for successful national development of AI.

Rules, standards, and R&D projects: Key areas for collaboration

Our exploration of international AI governance through roundtables, other discussions, and research led us to identify three main areas where enhanced collaboration would provide fruitful: regulatory policies, standard-setting, and joint research and development (R&D) projects. Below, we summarize ways in which cooperation may unfold in each of these areas, as well as the extent of collaboration conceivable in the short term as well as in the longer term.

Cooperation on regulatory policy

International regulatory cooperation has the potential to reduce regulatory burdens and barriers to trade, incentivize AI development and use, and increase market competition at the global level. That said, countries differ in legal tradition, economic structure, comparative advantage in AI, weighing of civil and fundamental rights, and balance between ex ante regulation and ex post enforcement and litigation systems. Such differences will make it difficult to achieve complete regulatory convergence. Indeed, national AI strategies and policies reflect differences in countries' willingness to move towards a comprehensive regulatory framework for AI. Despite these differences, AI policy development is in the relatively early stages in all countries, and so timely and focused international cooperation can help align AI policies and regulations.

AI policy development is in the relatively early stages in all countries, and so timely and focused international cooperation can help align AI policies and regulations.

Against this backdrop, it is reasonable to assume that AI policy development is less embedded in pre-existing legal tradition or frameworks at this stage, and thus that international cooperation in this field can achieve higher levels of integration. The following areas for cooperation emerged from the FCAI dialogues and our other explorations.

- **Building international cooperation into AI policies.** FCAI governments should give effect to their recognition of the need for international engagement on AI by committing to pursue coordination with each other and other international partners prior to adopting domestic AI initiatives.

- **A common, technology-neutral definition of AI for regulatory purposes.** Based on the definitions among FCAI participants and the work of the OECD expert group, converging on a common definition of AI and working together to gradually update the description of an AI system, and its possible configurations and techniques, appears feasible and already partly underway. A common definition is important to guide future cooperation in AI and determines the level of ambition that can be reached by such a process.

- **Building on a risk-based approach to AI regulation.** A variety of governments and other bodies have endorsed a risk-based approach to AI in national strategies and in bilateral or multilateral contexts. Most notably, a risk-based approach is central to the policy frameworks of the two most prominent exemplars of AI policy development—the U.S. and the EU. These recent, broadly parallel developments have opened the door to developing international cooperation on ways to address risks while maximizing benefits. However, there remain challenges to convergence on a risk-based approach. Dialogue on clear identification and classification of risks, approaches to benefit-risk analysis, possible convergence on cases in which the risks are too high to be mitigated, and the type of risk assessment to be performed and who should perform it, would greatly benefit cooperation on a risk-based approach.

- **Sharing experiences and developing common criteria and standards for auditing AI systems.** The field of accountability in AI and algorithms has been the subject of wide and valuable work by civil society organizations as well as governments. The exchange of good practices and—ultimately—a common, or at least a compatible, framework for AI auditing would eliminate significant barriers to the development of a truly international market for AI solutions. It also would facilitate the emergence of third-party auditing standards and an international market for AI auditing, with potential benefits in terms of quality, price, and access for auditing services for deployers of AI. Additionally, exchange of practices and international standards for AI auditing, monitoring, and oversight would significantly help the policy community keep up to speed in market monitoring.

- **A joint platform for regulatory sandboxes.** Even without convergence on risk assessments or regulatory measures, an international platform for regulatory learning involving all governments that participate in FCAI

and possibly others is a promising avenue for deepening international cooperation on AI. Such a platform could host an international repository of ongoing experiments on AI-enabled innovations, including regulatory sandboxes. As use of sandboxes becomes a more common way for governments to test the viability and conformity of new AI solutions under legislative and regulatory requirements, updating information on ongoing government initiatives could save resources and inform AI developers and policymakers. Aligning the criteria and overall design of AI sandboxes in different administrations could also increase the prospective benefits and impact of these processes, as developers willing to enter the global market might be able to go through the sandbox process in a single participating country.

- **Cooperation on AI use in government: procurement and accountability.** A natural candidate for further exchange and cooperation in FCAI is the adoption of AI solutions in government, including both "back office" solutions and more public-facing applications. The sharing of good practices and overall lessons on what works when deploying AI in government would also be an important achievement. Important areas in this respect are procurement and effective oversight of deployment.

- **Sectoral cooperation on AI use cases.** A sector-specific approach can ensure higher levels of regulatory certainty. In sectors like finance, key criteria such as fairness, discrimination, and transparency have long been subject to extensive regulatory intervention, and sectoral regulation must ensure continuity while accounting for the increasing use of AI. In health and pharmaceuticals, the use of AI both as a stand-alone solution and embedded in medical devices has prompted a very specific, technical discussion regarding the risk-based approach to be adopted and has already enabled valuable sectoral initiatives. The adoption of different standards and criteria in sectoral regulation may increase regulatory costs for developers willing to serve more than one sector and country with their AI solutions. In such a cross-cutting framework, examples from mature areas of regulation such as finance and health can also become a form of regulatory sandbox to model regulation for other sectors in the future.

Cooperation on sharing data across borders

Data governance is a focal area for international cooperation on AI because of the importance of data as an input for AI R&D and because of the added complexity of regulatory regimes already in place that restrict certain information flows, including data protection and intellectual property laws. Effective international cooperation on AI needs a robust and coherent framework for data protection and data sharing. There are a variety of channels addressing these issues including the Asia-Pacific Economic Cooperation group, the working group on data governance of the Global Partnership on AI, and bilateral discussions between the EU and U.S. Nonetheless, the potential impact of such laws on data available for AI-driven medical and scientific

research requires specific focus as the EU both reviews its General Data Protection Regulation and considers new legislation on private and public sector data sharing.

There are other significant data governance issues that may benefit from pooled efforts across borders that, by and large, are the subject of international cooperation. Key areas in this respect include opening government data including international data sharing, improving data interoperability, and promoting technologies for trustworthy data sharing.

Cooperation on international standards for AI

As countries move from developing frameworks and policies to more concrete efforts to regulate AI, demand for AI standards will grow. These include standards for risk management, data governance, and technical documentation that can establish compliance with emerging legal requirements. International AI standards will also be needed to develop commonly accepted labeling practices that can facilitate business-to-business (B2B) contracting and to demonstrate conformity with AI regulations; address the ethics of AI systems (transparency, neutrality/lack of bias, etc.); and maximize the harmonization and interoperability for AI systems globally. International standards from standards development organizations like the ISO/IEC and IEEE can help ensure that global AI systems are ethically sound, robust, and trustworthy, that opportunities from AI are widely distributed, and that standards are technically sound and research-driven regardless of sector or application.

International standards from standards development organizations like the ISO/IEC and IEEE can help ensure that global AI systems are ethically sound, robust, and trustworthy, that opportunities from AI are widely distributed, and that standards are technically sound and research-driven regardless of sector or application.

The governments participating in the FCAI recognize and support industry-led standards setting. While there are differences in how the FCAI participants engage with industry-led standards bodies, a common element is support for the central role of the private sector in driving standards. That said, there is a range of steps that FCAI participants can take to strengthen international cooperation in AI standards. The approach of FCAI participants that emphasizes an industry-led approach to developing international AI standards contrasts with the overall approach of other countries, such as China, where the state is at the center of standards making activities. The more direct involvement by the Chinese government in setting standards, driving the standards agenda, and aligning these with broader Chinese government priorities requires attention by all FCAI participants with the aim of encouraging Chinese engagement in international AI standard-setting consistent with outcomes that are technically robust and industry driven.

Sound AI standards can also support international trade and investment in AI, expanding AI opportunity globally and increasing returns to investment in AI R&D. The World Trade Organization (WTO) Technical Barriers to Trade (TBT) Agreement's relevance to AI standards is limited by its application only to goods, whereas many AI standards will apply to services. Recent trade agreements have started to address AI issues, including support for AI standards, but more is needed.

An effective international AI standards development process is also needed to avoid bifurcated AI standards—centered around China on the one hand and the West on the other. Which outcome prevails will to some extent depend on progress in effective international AI standards development.

R&D cooperation: Selecting international AI projects

Productive discussion of AI ethics, regulation, risks, and benefits requires use cases because the issues are highly contextual. As a result, AI policy development has tended to move from broad principles to specific sectors or use cases. Considering this need, we suggest that developing international cooperation on AI would benefit from putting cooperation into operation with specific use cases. To this end, we propose that FCAI participants expand efforts to deploy AI on important global problems collectively by working toward agreement on joint research aimed at a specific development project (or projects). Such an effort could stimulate development of AI for social benefit and also provide a forcing function for overcoming differences in approaches to AI policy and regulation.

Criteria for the kinds of goals or projects to consider include the following:

1. **Global significance.** The project should be aimed at important global issues that demand transnational solutions. The shared importance of the issues should give all participants a common stake and, if successful, could contribute toward global welfare.

2. **Global scale.** The problem and the scope of the project should require resources on a large enough scale that the pooled support of leading governments and institutions adds significant value.

3. **A public good.** Given its significance and scale, the project would amount to a public good. In turn, the output of the project should also be a public good and both the project and the output should be available to all participants and less developed countries.

4. **A collaborative test bed.** Governance of the project is likely to necessitate addressing regulatory, ethical, and risk questions in a context that is concrete and in which the participants have incentives to achieve results. It would amount to a very large and shared regulatory sandbox.

5. **Assessable impact.** The project will need to be monitored commensurately with its scale, public visibility, and experimental nature. Participants will need to assess progress toward both defined project goals and broader impact.

6. **A multistakeholder effort.** Considering its public importance and the resources it should marshal, the project will need to be government-initiated. But the architecture and governance should be open to nongovernmental participation on a shared basis.

This proposal could be modeled on several large-scale international scientific collaborations: CERN, the Human Genome Project, or the International Space Station. It would also build on numerous initiatives toward collaborative research and development on AI. Similar global collaboration will be more difficult in a world of increased geopolitical and economic competition, nationalism, nativism, and protectionism among governments that have been key players in these efforts.

Recommendations

Below, we present recommendations for developing international cooperation on AI based on our discussions and work to date.

R1. Commit to considering international cooperation in drafting and implementing national AI policies.

This recommendation could be implemented within a relatively short timeframe and initially would take the form of firm declarations by individual countries. Ultimately this could lead to a joint declaration with clear commitments on the part of the governments involved.

R2. Refine a common approach to responsible AI development.

This type of recommendation requires enhanced cooperation between FCAI governments, which can then provide a good basis for incremental forms of cooperation.

R3. Agree on a common, technology-neutral definition of AI systems.

FCAI governments should work on a common definition of AI that is technology-neutral and broad. This recommendation can be implemented in a relatively short term and requires joint action by FCAI governments. The time to act is short, as the rather broad definition given in the EU AI Act is still undergoing the legislative process in the EU and many other countries are still shaping their AI policy frameworks.

R4. Agree on the contours of a risk-based approach.

Alignment on this key element of AI policy would be an important step towards an interoperable system of responsible AI. It would also facilitate cooperation among FCAI governments, industry, and civil society working on AI standards in international SDOs. General agreement on a risk-based approach could be achieved in the short term; developing the contours of a risk-based classification system would probably take more time and require deeper cooperation among FCAI governments as well as stakeholders.

R5. Establish “redlines” in developing and deploying AI.

This may entail an iterative process. FCAI governments could agree on an initial, limited list of redlines such as certain AI uses for generalized social scoring by governments; and then gradually expand the list over time to include emerging AI uses on which there is substantial agreement on the need to prohibit use.

R6. Strengthen sectoral cooperation, starting with more developed policy domains.

Sectoral cooperation can be organized on relatively short timeframes starting from sectors that have well-developed regulatory systems and present higher risks, such as health care, transport and finance, in which sectoral regulation already exists, and its adaptation to AI could be achieved relatively swiftly.

R7. Create a joint platform for regulatory learning and experiments.

A joint repository could stimulate dialogue on how to design and implement sandboxes and secure sound governance, transparency, and reproducibility of results, and aid their transferability across jurisdictions and categories of users. This recommended action is independent of others and is feasible in the short term. It requires soft cooperation, in the form of a structured exchange of good practices. Over time, the repository should become richer in terms of content, and therefore more useful.

R8. Step up cooperation and exchange of practices on the use of AI in government.

FCAI governments could set up, either as a stand-alone initiative or in the context of a broader framework for cooperation, a structured exchange on government uses of AI. The dialogue may involve AI applications to improve the functioning of public administration such as the administration of public benefits or health care; AI-enabled regulation and regulatory governance practices; or other decision-making and standards and procedures for AI procurement. This recommended action could be implemented in the short term, although collecting all experiences and setting the stage for further cooperation would require more time.

R9. Step up cooperation on accountability.

FCAI governments could profit from enhanced cooperation on accountability, whether through market oversight and enforcement, auditing requirements, or otherwise. This could combine with sectoral cooperation and possibly also with standards development for auditing AI systems.

R10. Assess the impact of AI on international data governance.

There is a need for a common understanding of how data governance rules affect AI R&D in areas such as health research and other scientific research, and whether they inhibit the exploration that is an essential part of both

scientific discovery and machine learning. There is also need for a critical look at R&D methods to develop a deeper understanding of appropriate boundaries on use of personal data or other protected information. In turn, there is also a need to expand R&D and understanding in privacy-protecting technologies that can enable exploration and discovery while protecting personal information.

R11. Adopt a stepwise, inclusive approach to international AI standardization.

A stepwise approach to standards development is needed to allow time for technology development and experimentation and to gather the data and use cases to support robust standards. It also would ensure that discussions at the international level happen once technology has reached a certain level of maturity or where a regulatory environment is adopted. To support such an approach, it would be helpful to establish a comprehensive database of AI standards under development at national and international levels.

R12. Develop a coordinated approach to AI standards development that encourages Chinese participation consistent with an industry-led, research-driven approach.

There is currently a risk of disconnect between growing concern among governments and national security officials alarmed by Chinese engagement in the standards process on the one hand, and industry participants' perceptions of the impact of Chinese participation in SDOs on the other. To encourage constructive involvement and discourage self-serving standards, FCAI participants (and likeminded countries) should encourage Chinese engagement in international standards setting while also agreeing on costs for actions that use SDOs strategically to slow down or stall standards making. This can be accomplished through trade and other measures but will require cooperation among FCAI participants to be effective.

R13. Expand trade rules for AI standards.

The rules governing use of international standards in the WTO TBT Agreement and free trade agreements are limited to goods only, whereas AI standards will apply mainly to services. New trade rules are needed that extend rules on international standards to services. As a starting point, such rules should be developed in the context of bilateral free trade agreements or plurilateral agreements, with the aim to make them multilateral in the WTO. Trade rules are also needed to support data free flow with trust and to reduce barriers and costs to AI infrastructure. Consideration also should be given to linking participation in the development of AI standards in bodies such as ISO/IEC, with broader trade policy goals and compliance with core WTO commitments.

R14. Increase funding for participation in SDOs.

Funding should be earmarked for academics and industry participation in SDOs, as well as for SDO meetings in FCAI countries and more broadly in less developed countries. Broadened participation is important to democratize the standards making process and strengthen the legitimacy and adoption

of the resulting standards. Hosting meetings of standards bodies in diverse countries can broaden exposure to standards-setting processes around AI and critical technology.

R15. Develop common criteria and governance arrangements for international large-scale R&D projects.

Joint research and development applying to large-scale global problems such as climate change or disease prevention and treatment can have two valuable effects: It can bring additional resources to the solution of pressing global challenges, and the collaboration can help to find common ground in addressing differences in approaches to AI. FCAI will seek to incubate a concrete roadmap on such R&D for adoption by FCAI participants as well as other governments and international organizations. Using collaboration on R&D as a mechanism to work through matters that affect international cooperation on AI policy means that this recommendation should play out in the near term.

Proposed future topics for FCAI dialogues

- Scaling R&D cooperation on AI projects.
- China and AI: what are the risks, opportunities, and ways forward?
- Government use of AI: developing common approaches.
- Regulatory cooperation and harmonization: issues and mechanisms.
- A suitable international framework for data governance.
- Standards development.
- An AI trade agreement: partners, content, and strategy.

INTRODUCTION: AI AS A GLOBAL SOCIAL, ECONOMIC, AND STRATEGIC ISSUE

Rapid advancements in artificial intelligence (AI) over the past decade have produced explosive investment and development in AI. Both government and private funding for AI have increased, with global private investment rising to $67.9 billion in 2020.[1] In academia, the share of conference papers that focus on AI tripled from three percent in the late 1990s to nine percent in 2018. Forms of AI are being deployed in a wide variety of fields—most prominently, in biosciences, business analytics, and robotics—and AI increasingly is seen as a potentially transformative set of technologies across all sectors of the economy. AI, as a general purpose technology, could have wide-ranging economic impacts across manufacturing, transportation, health, education, and many other sectors.[2] In 2018, the McKinsey Global Institute estimated that AI could add around 16 percent, or $13 trillion, to global output by 2030.[3]

AI has also seen governments expand policymaking to harness the benefits of AI and manage risks to their economies and societies. In 2017, Canada became the first country to adopt an explicit national AI strategy. Now, according to the AI observatory maintained by the Organization for Economic Cooperation and Development (OECD), some 60 countries have AI initiatives.[4] Most of these national policies focus on investment in AI research and development (R&D) and talent to boost national competitiveness in the field. Other common elements include developing AI ethical principles, preparing the workforce for opportunities as well as disruptions from AI, and assessing the need for AI regulation and standards. Many national policies also espouse international cooperation as integral to maximizing the benefits of AI.

The seven governments involved are natural partners for this exploration. All are from countries that are strong in AI and are leaders in AI policy development.[5] Each government (except for Singapore) is an OECD member and has joined the OECD AI Principles. Each is participating in the Global Partnership on AI (GPAI), which is actively pursuing avenues of international cooperation.[6] All are linked across national security, trade, innovation, education, and more, at bilateral, regional, and multilateral levels. These relationships are built on common values that can guide fruitful development of AI governance that is open and accountable to citizens. Moreover, these governments collectively represent almost 50 percent of global GDP, as well as the majority of the world's AI research, talent, and commerce.[7] Each of them has demonstrated support for international cooperation through their national policies, the various international forums mentioned above, and their participation in the Forum for Cooperation on AI (FCAI).

This progress report presents an overview of the main findings of the activities carried out in the context of the FCAI and offers a number of preliminary recommendations, highlighting areas that will be subject to further exploration in the FCAI in the coming months.

Section 1 elaborates on the rationale for stronger international AI cooperation, highlighting attributes of artificial intelligence development that make it especially fit for broad cooperation and various domains that benefit from working together across borders: research and development, common principles of ethical and responsible AI, standards and regulations,

According to the AI observatory maintained by the OECD, some 60 countries have AI initiatives.

international trade and development, and the use of AI for good and in support of democracy and fundamental rights. In all these areas, we see a strong case for stepping up cooperation through a variety of channels and mechanisms.

Section 2 takes stock of the evolving landscape of international AI cooperation, both at the national and at the international level, in domains such as policy, regulation, and investment. AI policy around the world seems to have reached a tipping point, with governments now seeking ways to operationalize ethical principles into concrete policy provisions or detailed guidance for AI developers and deployers; at the same time, governments are also in the process of adapting their general AI framework and strategies to the specificities of individual policy domains and industry sectors. This tipping point presents a unique opportunity to strengthen international cooperation in AI policy and development while governments around the world are still in the early stages of understanding the issues and developing their approaches. Moreover, we see broad recognition that AI is of such magnitude in multiple dimensions that it requires nations to work together.

AI policy around the world seems to have reached a tipping point, with governments now seeking ways to operationalize ethical principles into concrete policy provisions or detailed guidance ... This tipping point presents a unique opportunity to strengthen international cooperation.

Section 3 identifies and describes specific areas where international cooperation on AI among governments and stakeholders would be fruitful. Based our analysis and ideas gleaned from the FCAI roundtables, we have so far identified three focal areas for such cooperation: regulatory policy, standards development, and collaborative R&D projects. Some are subjects for further exploration within the FCAI, while others are more suitable for other channels of cooperation.

Section 4 synthesizes the main findings of this report and distills the concrete recommendations to enhance international cooperation on AI regulatory policy, standards development, and large-scale R&D projects. We focus our recommendations on emerging issues as well as topics that will be explored in more detail in future FCAI roundtables.

1.

WHY INTERNATIONAL COOPERATION ON AI IS IMPORTANT

International cooperation is key to realizing the benefits of AI and addressing its risks. On one hand, no one country acting alone can make ethical AI pervasive, leverage the scale of resources needed to realize the full benefits of AI innovation, and ensure that the advances from developing AI systems can be made available to users in all countries in an open and nondiscriminatory trading system. On the other hand, the opportunity cost of insufficient international cooperation is further exacerbated by the prospect of uncoordinated regulatory interventions that would limit opportunities for R&D, create costs to AI use and investment, and undermine the capacity for FCAI-participating governments to establish a system of AI governance built on democratic principles and respect for human rights. This latter issue also is gaining strategic importance given China's growing leadership in AI combined with its authoritarian government, which inevitably promotes an approach to AI development that is less grounded in the protection of the democratic process and associated values.

In the field of R&D, international collaboration has proven to create economies of scale and scope, generate benefits due to complementarity and coupling of funding sources, "enhance diffusion of ideas," and "institutional incentives and subsidies."[8] Collaboration in R&D can also contain logistical challenges, either due to a lack of coordination, errors, or reputational risks.[9] In regard to international standardization, there is a consistent stream of academic literature showing positive effects on GDP, labor productivity, and growth.[10] The OECD has been very active over the past decade in analyzing the benefits and potential risks of international cooperation, especially from a regulatory perspective.[11] The benefits of regulatory cooperation include, notably, the establishment of a level-playing field for international trade and competition, which in turn avoids "races to the bottom" with countries competing to attract investment by adopting more lenient regulatory frameworks. In addition, multilateral cooperation can be beneficial especially for smaller countries that lack the economic weight to develop and adopt their own standards.[12]

At the same time, these benefits are dependent on the creation of effective and efficient frameworks for cooperation, as well as the adoption of an optimal level of cooperation. In turn, cooperation can develop to different extents, and at different levels, and preservation of specific features in national strategies can also be beneficial in that they allow for mutual learning across countries. Below, we identify how these benefits of international cooperation play out in several domains of AI development and policy. These areas include investing in R&D pursuing ethical, trustworthy, and reliable AI development; defining rules and standards for AI; establishing an open and effective trade policy framework; tapping the potential of AI for good; and addressing challenges posed by China's emerging prominence in the AI landscape. Like the work of FCAI so far, this report is focused on identifying areas for international cooperation, aligning regulation and standards where possible, and minimizing barriers to AI development and dissemination.

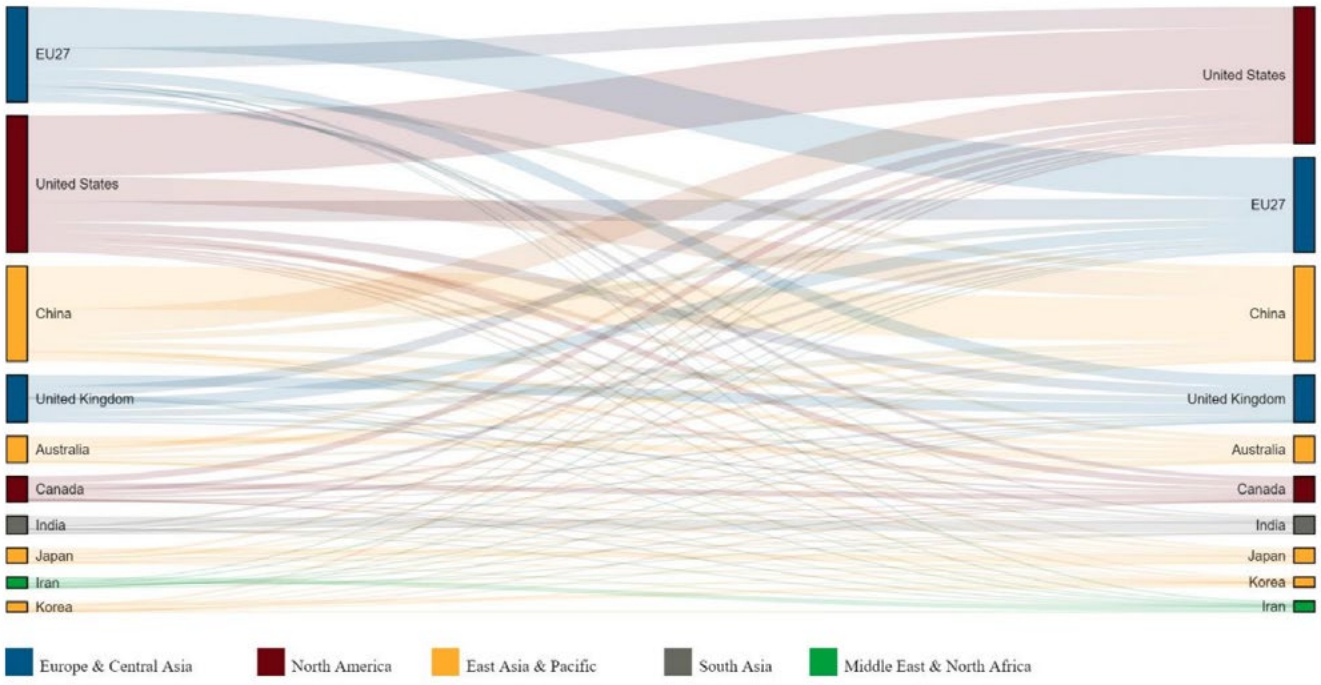
1.1. Promoting AI research and development

AI is an increasingly complex and resource-intensive research effort in which scale offers an important advantage. Cooperation among researchers and developers across national boundaries can create expanded opportunities to realize economies of scale and to exploit comparative advantages for mutual benefit. Conversely, an absence of international cooperation can lead to lack of knowledge sharing as well as duplicative investments in AI infrastructure and capacity, creating unnecessary costs and leaving each country worse off in terms of AI outcomes.

Not surprisingly, therefore, collaboration in AI R&D across national borders has been very strong and appears to be growing further. One analysis found that such cooperation has become more common over time citing that as of 2019, 27.8 percent of AI papers were published by international research teams.[13] The same analysis concluded that "the U.S., the U.K., France, and Spain led global collaboration research in the field of AI." China, too, plays an active role in international collaboration in AI research with around 3,000 AI papers jointly authored between Chinese researchers and researchers from the U.S., EU, Australia, Canada, or Japan in 2018.[14]

Figure 1 from the Organization for Economic Cooperation and Development (OECD) on joint publications on AI across borders illustrates how interwoven these research networks are.

Figure 1. Domestic and international AI research collaboration



Source: OECD.ai (2021)[15]

This high level of collaboration and the scale of development highlight the particular economies of scope and scale that apply to R&D for AI. AI R&D requires a number of key inputs that can be synergized and more efficient at an international scale:

This high level of collaboration and the scale of development highlight the particular economies of scope and scale that apply to R&D for AI. AI R&D requires a number of key inputs that can be synergized and more efficient at an international scale.

- **Access to high-quality data.** The current focus of AI on supervised machine learning leads to prioritizing access to large, labeled data sets. For this reason, in large part, many government strategies identify access to data as a key priority.[16] Enhancing R&D cooperation through sharing large-scale, high-quality public and private data sets can significantly contribute to progress in AI across numerous applications, including AI for good, and may require well-framed environments for collaboration in the context of public-private research projects (see Section 3.3 on page 69). Providing researchers with a stable and reliable framework for access to data globally for research purposes is as essential as it is complicated, especially due to the current fragmentation in regulations concerning data protection and governance (see below). In addition, the emergence of standards in the research community and standards bodies on data management and governance practices can support international collaboration in AI R&D.[17]

- **Sharing the cost of large-scale computing infrastructure.** With the computing power and infrastructure needed to run cutting-edge AI algorithms becoming increasingly costly, computing capacity is another key requirement for AI development.[18] For example, a recent paper from OpenAI reports that computing power in the largest machine learning experiments doubles every 3.4 months, an elevenfold increase each year.[19] Other estimates have suggested that advanced AI model training can cost between tens of thousands to over a million dollars.[20] To help many smaller research groups advance AI and its applications within their respective fields, researchers need more access to massive computing power through development of supercomputing centers, research clouds, and distributed computing networks. CERN (formally the Conseil Européen pour la Recherche Nucléaire, or European Center for Nuclear Research), for example, has demonstrated the opportunities from international collaboration on computing capacity through development of the Worldwide LHC Computing Grid, a network of 170 computing centers in 42 countries, to handle the large volume of data generated by its Large Hadron Collider.

- **Knowledge.** Today, scientific research is a broad global enterprise that relies on collaboration and shared resources. In AI, the underlying programming languages used most often are largely open-source and rely on international collaboration for their development. Many of the most powerful AI packages are openly available (e.g., TensorFlow, PyTorch, scikit-learn, and tidymodels); and trained models such as OpenAI's GPT-3 for language and VGG16 or Inception for image classification are available for reuse for specific tasks through a process called transfer learning.[21] AI R&D also relies on knowledge that is widely and rapidly shared as a majority of AI papers appear as preprints on arXiv or other public websites even before their formal presentation at conferences, which is thought to have significantly increased the pace of information

sharing, and through that, discovery. Many applied projects also release code, often on the code-hosting website GitHub, enabling it to be replicated, augmented, and adapted for other purposes.

- **Talent.** AI R&D often involves multidisciplinary teams in multiple locations, different organizations, or research institutions that rely heavily on open-source software, shared data, and distributed computing. This open and distributed approach to AI innovation has allowed researchers from China to Australia to India to gain and transfer AI skills, thus contributing to global AI innovation.[22] In turn, policies that reduce this global exchange of ideas and research projects—such as restricting the travel or collaboration of researchers (through restrictions on immigration or export controls), sharing of research results (through controls on dissemination of information), limiting the flow of data (through restrictive data governance regimes or extensive data localization requirements)—can reduce the ability to collaborate in R&D and acquire talent and knowledge, and thereby reduce the pace of global AI development.[23]

1.2. Affirming democratic principles for trustworthy AI

Broad expression of democratic values has been a common element of numerous AI and technology policy statements by governments, multilateral organizations, and other bodies. The G-7's Carbis Bay Summit Communiqué called for coordination "to ensure that the use and evolution of new technologies reflect our shared democratic values and commitment to open and competitive markets, strong safeguards including human rights and fundamental freedoms." Within this context, there is wide agreement on broad principles for trustworthy and human-centered AI. Forty-two countries have now signed onto the AI principles of the Organization for Economic Co-operation and Development (OECD), which include respect for the rule of law, human rights, and democratic values.[24] The OECD principles are particularly important since they are referenced by the G-20's AI principles and the OECD has become the supporting office for the Global Partnership on AI.[25]

In particular, ethical principles for AI development, deployment, and use have also been a focus of frameworks introduced by technology companies, professional bodies, standards organizations, governments, and researchers. Among others, the nonprofit AlgorithmWatch has built an inventory of AI Ethics Guidelines updated as of April 2020, which already featured 173 documents;[26] and the Council of Europe has developed a database of 450 policy initiatives on AI, mostly related to human rights and responsible AI development.[27] While there are far too many AI ethics principles and frameworks to discuss them all here, a few stand out. The Asilomar AI Principles, developed in 2017, were signed by nearly 6,000 AI experts and adopted as informal guiding principles by the state of California.[28] The IEEE's Ethically Aligned Design is a comprehensive exploration of AI developed

over a three-year period, also involving several thousand experts.[29] AI Now was an early civil society mover in propounding recommendations for government policies.[30]

There is considerable overlap among these various sets of principles, including on the importance of fairness, privacy preservation, and respect for human rights and autonomy. An analysis of 22 AI ethics principles found that the values of accountability, privacy, fairness, transparency, and cybersecurity appeared in over 70 percent of the documents. Other common principles include human oversight, explainability or interpretability, legal status of AI systems, and the equitable economic effect of AI.[31] A separate analysis of 84 AI ethics documents done in 2019 found that there has been a global convergence around "transparency, justice and fairness, non-maleficence, responsibility and privacy."[32]

The next step toward AI governance is to translate AI principles into policy, regulatory frameworks, and standards.

While much progress has been made aligning on responsible AI, there remain differences—even among FCAI participants. Further alignment on approaches to AI is an important step toward building international AI cooperation (see Section 3.1 on page 44). The enhanced global diffusion from cooperation on AI ethical principles can guide AI policies among likeminded countries and influence machine learning engineers and technology sector CEOs to incorporate better AI practices, and also attract the scrutiny of journalists, consumers, and regulators as they seek to hold AI systems accountable. Ethical guidance may also steer the attention of public and private research; there likely is some mutual reinforcing effect of the stated importance of risk assessment, transparency, interpretability, explainability, robustness, and privacy on technical advances in AI research.

The next step toward AI governance is to translate AI principles into policy, regulatory frameworks, and standards. This will require deeper understanding of how AI works in practice and working through the operation of principles in context and inevitable tradeoffs, such as may arise when seeking AI that is both accurate and explainable. Effective cooperation will require concrete steps in specific areas, which the recommendations of this report aim to suggest.

1.3. Developing consistent AI regulation, standards, and conformity assessment practices

Without international cooperation, divergent approaches to AI regulation can create barriers to AI innovation and diffusion even with agreement on AI values and principles. Moreover, government efforts to boost domestic AI development around themes of digital sovereignty can have negative spillover effects, such as restrictions on access to data, data localization, discriminatory investment, and other compliance requirements.[33] International cooperation is needed here to address risks of protectionism and avoid fragmentation and trade tensions that limit the global potential of AI.

In contrast, AI regulation that is aligned and interoperable can not only reduce market barriers but also strengthen oversight and raise trust in AI. International alignment on AI regulation can reduce scope for regulatory arbitrage by governments and AI providers that leads to a race to the bottom, which would undermine the objectives that these and similarly-minded countries seek for AI. Cooperation on how governments use AI can also enhance AI governance. This includes leveraging their purchasing power as major users of AI systems in areas ranging from national security and law enforcement to R&D, education, and delivery of social services.

Regulatory divergence can also be expensive. For instance, the OECD estimated in 2018 that regulatory divergence costs the global financial services industry around US$780 billion per year, which amounts to between five to 10 percent of the annual turnover of financial institutions.[34] Varying governmental AI regulations will require developers to build different AI models for each market, thus increasing the amount of work necessary to build an AI system, and leading to higher consumer costs. Different regulations also may force variation in how data sets are collected and stored, creating additional complexity in data systems and reducing the general downstream usefulness of the data for AI.

Additional costs and barriers from different AI regulations are especially problematic for smaller firms. Larger established companies have more resources for technical staff and legal experts to adapt to varying regulatory barriers. Large technology companies already have the advantage of access to big data and large-scale AI systems, and thus regulation should be especially careful not to add burdens to smaller companies and entrepreneurs. This has been a problem in the past, as in the case of widely praised policy interventions such as the EU General Data Protection Regulation (GDPR). For instance, Google's and Facebook's ad revenue appears to have been less impacted by GDPR than smaller ad companies.[35] In the financial services industry, the OECD has estimated that international regulatory divergence is materially more costly to smaller firms than to larger ones.[36]

Correspondingly, international regulatory alignment has value for specialized firms in AI development. Such companies generate business by developing expertise in a specialized AI model, then selling or leasing these to other companies as part of a broader tool. As AI becomes more ubiquitous, complex stacks of individual, specialized AI systems may exist in many products. A more open global market would allow a company to take advantage of digital supply chains. For example, using a single product with a natural language processing model built in Canada, a video analysis algorithm trained in Japan, and network analysis developed in France. Enabling global competition by these specialized firms will lead to healthier markets and greater AI innovation.

1.4. Facilitating international trade and investment

Cooperation on AI will facilitate an open, nondiscriminatory trading system by enabling commitments in trade agreements to align domestic AI regulation by applying international AI standards and cooperating on measures such as conformity assessment and labeling. Trade policy, in turn, can underpin international cooperation to enable global data flows, including in ways that ensure strong privacy and security.[37] This includes a need for international cooperation to address barriers to data access as a result of restrictions by governments on data flows and data localization requirements. Trade policy could also support international cooperation on AI by incentivizing cooperation on cybersecurity, supporting cross-border innovation, and reducing barriers and costs to AI infrastructure.

In addition to using trade and investment policy to expand opportunities for AI, cooperation among FCAI governments is needed to effectively reduce access by nondemocratic governments to specific AI-related technologies that can undermine the goal of building responsible global AI governance or conflict with collective security interests. Here, export controls and foreign investment screening regimes, often for competitive and national security reasons, can limit access to AI technologies—thus requiring careful international cooperation to maximize the national security effectiveness of such restrictions among trading partners and allies while also avoiding overreaching or stifling legitimate international AI investment.

1.5. Deploying AI for global good

The governments involved in the FCAI share interests in deploying AI for social, humanitarian, and environmental benefits around the world. For example, the EU's recent Data Strategy proposed to employ AI to support its Green New Deal, and the G-7 has called for harnessing AI to boost progress on the U.N. Sustainable Development Goals (SDGs).[38] These aims involve challenges on a global scale and require public investment on a commensurate scale. They also are public goods that are unlikely to be supplied by the private sector.

The opportunities in these veins present a clear case for cooperation among governments in order to reach the scale required to have a global impact and to take advantage of AI. Many of the SDGs are grounded in expanding access to technology. Collaborative projects between data scientists and public service organizations show how AI can be used to improve traffic safety, help public assistance reach people in need, and better optimize medical care.[39] The Future Society has also identified a number of these projects, which include efforts to use drones to find landmines and to tackle modern slavery.[40] International collaboration can benefit by highlighting successful interventions and providing funding to expand their scope across borders.

1.6. Addressing the China challenges on AI

China is a leading global economy as well as a preeminent leader in the field of AI and related technologies. It is also a leading trade partner with all FCAI participants, which depend on China for their supply chains and valuable export markets. In principle, China could be an attractive partner in AI. Chinese researchers are performing cutting edge work and, by some measures, lead the world in patents and publications related to AI. Furthermore, China has developed its own AI ethical principles that align with Western ethical principles in material ways.[41] Yet, China's social and economic control presents democratic countries with distinct challenges that place its development and deployment of AI in sharp relief.

China's use of technology on a vast scale to monitor and score the Chinese population, and specific subgroups, and its willingness to export surveillance technologies to other authoritarian governments[42] are at odds with democratic values. In particular, this application of AI is in tension with human dignity and autonomy as well as individual rights of freedom of expression and nondiscrimination.

This authoritarianism is linked to other policies that threaten to splinter the internet and the AI world along different technology standards and markets. President Xi Jinping has affirmed China's goals for AI (and other strategic technologies) as reducing "external [foreign] dependence for key technologies and advanced equipment."[43] This goal has been carried out through an array of laws and policies that include strict national security controls for communications technology and internet services, extensive government subsidies for national AI champions, aggressive acquisition of foreign intellectual property by covert as well as open means, and barriers to competition from FCAI participants and others. China's political and economic autarky converge in its deployment of the Great Firewall for internet communications and of facial recognition surveillance to wall in its population and wall out unwanted foreign intercourse. The sheer size of its population and economy makes it feasible for China to adopt this forked approach to development for the indefinite future.

A cooperative framework centered on common values would provide a strong counterpoint to China's development of AI as an instrument of its authoritarian capitalism and to its forking of the global internet. This does not have to mean shutting the door on cooperation with China on AI issues.[44] Rather, it requires accepting Chinese progress in AI in certain domains, working to constrain threats where feasible and to shape approaches where possible.[45] China's AI scientists have much to contribute as genuine partners to global AI R&D—and China as a whole is a needed partner in addressing global problems.

China's use of technology on a vast scale to monitor and score the Chinese population ... and its willingness to export surveillance technologies to other authoritarian governments are at odds with democratic values.

However, such engagement with China cannot be compartmentalized as "just business," without regard to concerns about values, ethics, and democratic principles. For governments, enterprises, and other organizations in democratic countries, doing business with China under its current policies will need to be undertaken with eyes wide open to an array of risks and

compromises. In the end, the digital world may be divided into different systems. Democratic governments should work to discourage this, but also prepare for the possibility by ensuring that the systems they rely on are collaborative and trustworthy, including with respect to AI.

2.

MAPPING THE TERRAIN: NATIONAL AND INTERNATIONAL DEVELOPMENTS

Exploring ways to step up international collaboration in AI requires an understanding of where countries stand in their own national strategies and initiatives, as well as an exploration of the existing forums and platforms for dialogue and standard-setting in the domain of AI. In this section, we take stock of existing developments starting with national strategies and policies among FCAI participants (Section 2.1) and then moving to analysis of the international landscape for AI cooperation and standard-setting (Section 2.2). Table 1 following Section 2.1 summarizes developments among the governments participating in FCAI. This table compiles a range of data on each country's AI investment, AI policies, and development of an approach to AI standards. Due to differences in how countries report data, as well as our focus on the EU rather than member states, this table presents a snapshot of AI activity but is imprecise in terms of making cross-country comparisons.

2.1. National developments among FCAI participants

Australia

Australia's artificial intelligence roadmap, published as Artificial Intelligence, proffers three high-level strategic focuses for the country's approach to AI. These include specialization to capitalize on comparative advantages, mission-directed research aimed at addressing critical issues, and the mapping of business and knowledge ecosystems to "leverage networks of expertise and resources which lie across jurisdictional boundaries." Considering Australia's current capabilities and comparative advantages, the roadmap specifies three "high-potential" areas of AI specialization: (1) health, aging, and disability, (2) cities, towns, and infrastructure, and (3) natural resources and the environment. The report clarifies that its emphasis on these areas is not meant to stifle innovation in other sectors, but rather that AI development in the targeted sectors will benefit Australia domestically and provide opportunities for global export. Furthermore, the roadmap identifies a need for between 32,000 and 161,000 AI specialist workers by 2030, as well as effective data governance, high standards, and transparency to ensure public trust.[46]

In June 2021, Australia released an AI Action Plan as a "key feature" of the government's Digital Economy Strategy which, for the 2021–2022 budget, includes a US$90 million investment into the creation of a National Artificial Intelligence Center, public-private partnerships, AI workforce development, and grants to develop AI solutions for local or regional challenges.[47]

Australia has not adopted laws that specifically regulate "AI, big data, or algorithmic decision-making."[48] However, as noted in the AI Action Plan, the Australian government has taken steps to ensure progress in AI is responsible and inclusive by releasing Artificial Intelligence: Australia's Ethics Framework in 2019, aligning itself with the values outlined in the OECD Principles on AI.[49] Following quickly in 2020, Standards Australia published An Artificial Intelligence Standards Roadmap: Making Australia's Voice Heard, which included recommendations to increase engagement

with international standards-setting bodies, such as in the International Organization for Standardization and International Electrotechnical Commission Joint Technical Committee 1 for Information Technology (ISO/IEC/JTC 1/SC 42) .[50] Reflecting these recommendations, the AI Action Plan promises to "review existing regulations and develop meaningful guidance on the sharing and use of data," specifically referencing the Privacy Act of 1988, the Data Availability and Transparency Bill of 2020, and the forthcoming Australian Data Strategy.[51] Australia's AI Action Plan also affirms the country's commitment to internationality in the context of AI, noting its participation in the Global Partnership on AI (GPAI), international standards-setting, and the broader implementation of its International Cyber and Critical Technology Engagement Strategy.[52]

Canada

With over 20 public research labs, 850 startups, and 75 incubators, Canada's public and private sectors have made AI research and development a centerpiece of Canada's AI strategy. The Canadian government directed the Canadian Institute for Advanced Research (CIFAR), a nonprofit research organization, to launch a program, the comprehensive Pan-Canadian AI Strategy in 2017, the first comprehensive national strategy worldwide, which set goals to recruit and train AI researchers in Canada and promote AI R&D.[53]

Since then, the CIFAR Pan-Canadian AI Strategy has established three AI research centers (which have hosted graduate students and senior AI researchers worldwide, and funded CIFAR AI R&D grants on a range of topics). The CIFAR Pan-Canadian AI Strategy received an initial investment of C$125 million over five years from the Canadian government, the Royal Bank of Canada, and Facebook; the 2021 budget proposes to renew government funding for C$444 million over 10 years.[54] Building on these partnerships, the private sector has established over 45 AI R&D labs in Canada since 2017; Montreal, in particular, has received about C$900 million in foreign direct investment since 2017 and almost C$1 billion in public funding to support AI projects.[55] In 2018, the Université de Montréal, in collaboration with the Fonds de recherche du Québec, circulated the Montréal Declaration for a Responsible Development of AI after broad consultations with experts in government, industry, and civil society.[56] It provides ethical guidelines and recommendations to address various risks in designing and implementing artificial intelligence, including privacy protections, control over personal information, audits, and publicly accessible decisionmaking algorithms.

In addition, Canada has issued regulations to address certain risks related to artificial intelligence and the processing of personal information in the federal government; the Directive on Automated Decision-Making came into effect April 19, 2019, requiring federal government bodies to complete algorithmic impact assessments prior to utilizing automated decisionmaking tools, notify affected parties both before and after automated decisions, and analyze all results for potential bias.[57] In the private sector, the federal Personal Information Protection and Electronic Documents Act (PIPEDA) regulates how businesses handle personal information, setting out ten fair information principles that include safeguards to maintain privacy, accuracy, and fairness in data processing and minimize potential harms or discrimination to

individuals.[58] These regulations—together with Canada's Digital Charter, a government initiative to build public trust in emerging technologies—contribute to the government's objectives to maximize the economic and social benefits of AI while minimizing any potential pitfalls or risks.[59]

Canada has made working with the international community on collective ways to harness the benefits of AI a feature of its AI strategy.

Canada has made working with the international community on collective ways to harness the benefits of AI a feature of its AI strategy. Canada co-led the formation of the Global Partnership on Artificial Intelligence (GPAI) within the G-7 along with France.[60] Navdeep Bains, Canada's minister of innovation, science, and industry highlighted the focus on international cooperation during GPAI's opening ceremonies: "Realizing the full potential of AI by creating benefits for all citizens requires international collaboration and coordination. GPAI will help shape a global AI ecosystem where innovation and growth are founded on trust and harnessed by our shared values of human rights, inclusions, and diversity."[61]

In 2019, the federal government also established the Advisory Council on AI to advise on domestic and international AI standards, carry out the Digital Charter, and support Canada's collaboration with the international AI community, including with the G-7, the G-20, the OECD, and the World Economic Forum. [62] It announced a bilateral initiative with the United Kingdom in 2020, allocating C$5 million over three years to fund joint research on a range of AI use cases including identifying global public health crises, improving smart transportation, and curtailing online harassment.[63]

European Union

The European Commission embarked on its AI strategy in 2018 with a Coordinated Plan on Artificial Intelligence,[64] along with the establishment of a High-Level Expert Group on AI[65] and launch of a multistakeholder AI Alliance. As 21 out of 27 EU member states had published national AI policy documents[66] outlining country-specific priorities, recommendations, R&D resources, and national funding, the European Commission acted to ensure a well-functioning European internal market for AI systems; in 2019 it adopted a data strategy and in 2020, an influential white paper on AI.[67] These outline the EU's ambition to create an innovation-friendly "ecosystem of excellence" and a human-centric "ecosystem of trust" in AI.

On this foundation, the European Commission published a revised Coordinated Plan on Artificial Intelligence (referred to as Coordinated Plan)[68] in April 2021 which aligns national, European, and global AI initiatives aimed at making the EU a leader in AI and the setting of global norms. The plan's centerpiece is the Artificial Intelligence Act, a legislative proposal on regulatory requirements for certain AI systems.[69] This legislation proposes a risk-based regulatory framework aimed at specific uses of AI that create risks to safety or to EU fundamental rights. It introduces four categories of risk (unacceptable risk, high risk, limited risk, and minimal risk) and bans certain AI systems (social scoring and biometric identification in health care, transport, policing, and the judiciary) in the EU digital single market. This risk-based approach limits application only "where strictly needed and in a way that minimizes the burden for economic operators, with a light governance structure" but, for all AI systems classified as high risk, sets a high bar with detailed rules related

to data quality and traceability, transparency and human oversight, and conformity assessments.[70] The AI Act will be enforced both at the member state and European Union level by a newly established European Artificial Intelligence Board.[71]

The EU plan includes additional measures in support of innovation, such as AI regulatory sandboxes and access to testing and experimentation facilities, as well as "Digital Innovation Hubs," networks of "AI Excellence Centres" and a controlled testing environment for established businesses, small and medium sized enterprises, and start-ups.[72] Through the research and innovation investment programs Horizon 2020, Horizon Europe, and a "Recovery and Resilience Facility," the EU plans to invest around €1 billion yearly and up to €20 billion until 2030 into AI, in addition to funding for various digital technologies, and cybersecurity.[73] The EU conceives of AI as part of a wider EU digital governance ecosystem that encompasses the EU data strategy, GAIA-X cloud project, Digital Services Act, Digital Markets Act, Cybersecurity Strategy, Digital Compass 2030 White Paper, and a public consultation on a set of European digital products[74]—all aimed at shaping additional resolutions by the European Parliament and the parliament's ongoing work in the Special Committee on AI in a Digital Age and Centre for AI.[75]

At the international level, the EU aims to lead international norms for development and deployment of trustworthy AI. The Coordinated Plan announces "actions to foster the setting of global AI standards in close collaboration with international partners in line with the rules-based multilateral system and the values it upholds."[76] Despite the comparatively strict regulatory requirements proposed for high-risk AI systems operating in the EU market, the AI Act states that "the proposed minimum requirements are already … largely consistent with other international recommendations and principles, which ensures that the proposed AI framework is compatible with those adopted by the EU's international trade partners."[77] EU-led initiatives include the international multistakeholder AI Alliance, and the recently launched U.S.-EU Trade and Technology Council, in which AI is a focus of one of several working groups on digital trade and policy issues.[78]

Japan

Japan's AI ecosystem draws from a traditionally impactful R&D and technology sector. An integral element of its AI governance is its Society 5.0, a conceptual vision document guiding actions in science, technology, and innovation aimed at synergies for a prosperous future.[79] The Society 5.0 framework frames Japan's AI principles (human-centricity, education/literacy, privacy, security, fair competition, fairness, accountability and transparency, and innovation) mainly in relation to cultural and social aspects of its society.[80] The Cabinet Office Council on Industrial Competitiveness[81] has targeted self-driving cars, drones, and production management, including smart factories, all powered by AI, as key opportunities to increase Japan's productivity. Public Japanese research institutes such as the National Institute of Advanced Industrial Science and Technology (AIST) and Institute of Physical and Chemical Research the Institute of Physical and Chemical Research (RIKEN) also contribute to AI innovation by establishing new R&D centers to speed up technological advancements in relation to AI technology.

Japan describes its "ideal approach to AI governance" as a set of "non-binding intermediate goal-based guidelines to promote AI innovation and deployment."[82] Under the approach, risk management should be commensurate with the context and size of an organization and "legally-binding horizontal requirements for AI systems are deemed unnecessary at the moment."[83] Pursuant to this approach, the government has issued a number of guidelines to guide AI stakeholders including researchers, businesses, and the public: R&D Guidelines (2018),[84] Social Principles of Human-Centric AI (2019),[85] and AI Utilization Guidelines (2019).[86]

The AI R&D Guidelines and AI Utilization Guidelines have contributed significantly to the development of international AI policy frameworks, most notably the international OECD AI Principles.[87] Japan's Ministry of Economy, Trade and Industry (METI) puts the Japan's AI principles at the core of their strategic objective to advance international cooperation on AI and digital technologies more generally. Picking up where Canada's presidency left off, Japan's G-7 presidency was instrumental in the launch of GPAI. Likewise, the further development of Japan's Data Free Flow with Trust (DFFT) framework, which enables multilateral data transfers between countries, was a focus of the G-7 in the Japanese presidency. The World Economic Forum has taken up the banner of the DFFT framework, and Japan recently co-hosted the Global Technology Governance Summit (2021)[88] with the World Economic Forum (WEF) to promote international cooperation and data flows. Looking ahead, METI considers the implementation of its guidelines, public sector use of AI, international harmonization of AI governance frameworks, as well as "coordination between policies and standards," as key issues in the field of AI governance.[89]

Singapore

Artificial intelligence and emerging technologies play a central role in the Singaporean government's plan for economic growth—demonstrated through its "Smart Nation" initiative to expand the digital economy.[90] Singapore released its National AI Strategy in November 2019, outlining the government's plans to prioritize AI research in transportation, smart cities, health care, education, and security, as well as to facilitate access to the datasets, resources, and workforce necessary to support AI advancements.[91] Within this strategy, the government affirms that "international collaboration is essential for driving sustainable development of AI" and pledges to partner with international organizations and the private sector to devise AI standards and advance research.

As part of the National AI Strategy, the government encourages public-private research collaborations, including with private companies that operate globally as well as domestically within Singapore. Singapore has designated over S$500 million for AI research through its RIE2020 Plan, and plans to allocate S$200 million to improve supercomputing and network infrastructure.[92] In addition, the government's National Research Foundation has pledged to invest up to S$150 million in AI research, development, and adoption through the AI Singapore (AISG) program.[93] Toward these goals, AISG has encouraged public-

private research collaborations and is working with research institutions, start-ups, corporations, and academics to share software, open-source datasets, and other resources and tools.

Although it has not yet enacted laws specific to AI ethics or risks, the Singaporean government passed revisions to the Personal Data Protection Act (PDPA) in 2012. This law governs how most businesses operating in Singapore treat personal information and prohibits data transfers to countries without comparable protections. Like the GDPR and other similar laws, the PDPA could affect AI development and adoption in Singapore—it could help businesses limit the privacy and data protection risks of automated systems but also pose implications for the data transfers and flows that are essential to their creation.

In addition, Singapore has released nonbinding guidance to help organizations navigate data ethics and governance principles, such as transparency, fairness, and explainability. It developed the Trusted Data Sharing Framework[94] in 2019 to help foster a nascent data sharing ecosystem by guiding companies and nongovernmental organizations through trust and security considerations of data exchanges.[95]

Singapore has released nonbinding guidance to help organizations navigate data ethics and governance principles, such as transparency, fairness, and explainability.

The same year, Singapore also released its Model AI Governance Framework, which outlines how AI systems work, how to reduce bias in AI applications, and how to facilitate open and transparent communication.[96] Singapore's Model AI Governance Framework is framed broadly to apply to a range of technologies, sectors, and business models, providing guidance in areas such as how to identify and address risks associated with AI adoption, such as accuracy and bias. Like the EU Ethics Guidelines for Trustworthy AI, Singapore's framework also offers suggestions on the levels of human oversight necessary to mitigate any potential risks from adoption. The framework was updated in 2020 and is accompanied by an Implementation and Self-Assessment Guide and a Compendium of Use Cases, demonstrating how various organizations applied the framework in their AI systems' business operations. In doing so, Singapore's vision for AI governance demonstrates that accountable AI practices and beneficial use of AI in business are not mutually exclusive.

United Kingdom

The United Kingdom (U.K.) and its flourishing technology and R&D ecosystem consider AI pivotal to the country's overall policy agenda. Several U.K. government offices shape AI governance: a specialized Office for AI oversees implementation of the national AI strategy, called the AI Sector Deal.[97] The U.K. government's budget of £0.95 billion for the AI Sector Deal is in addition to £1.7 billion allocated through the Industrial Strategy Challenge Fund. This funding is part of the U.K.'s strategic objectives in support of AI innovation in the priority areas of advanced health care and treatment, automation of potentially life-threatening and dangerous jobs, and skill-building for the future workforce. The AI Council, an independent committee advising the Office for AI, published an AI Roadmap in 2021, with contributions from industry, academia, and civil society. It names the Alan Turing Institute as the national AI research center to "remain a globally leading player in AI," "promote the U.K.'s interests through collaborations with international partners," and "attract world-leading talent to the U.K.."[98]

The Centre for Data Ethics and Innovation, an independent advisory body set up and tasked by the U.K. government, investigates and advises on a sustainable, safe, and ethical use of AI. The Centre also refers to the guide to using AI in the public sector,[99] a specific goal of the U.K. AI governance objectives. The U.K. strategy does not mention the introduction of specific legislation but suggests a need to provide legal certainty for data sharing, data usage, and data protection. In September 2021, the government launched a consultation with a proposed "new direction" to consider revisions to the U.K.'s Data Protection Act (which mirrors the EU's GDPR) in ways that could enable greater data sharing.[100]

International cooperation in AI is a key objective for the U.K.. The AI Roadmap describes the combination of the U.K.'s research leadership with its "diplomatic weight" as "a catalyst to shape international discussions."[101] As the 2021 G-7 president, the U.K. made cooperation in AI a focus of the 2021 Summit—demonstrated by the expressed aim of the Carbis Bay G-7 Summit Communiqué "to rally all partners around our open and human centric approach to artificial intelligence" and looking to the GPAI November, 2021 Summit in Paris"[102] to contribute to "government-to-government dialogue" on AI and strengthen cooperation on a common AI R&D ecosystem and public-private partnerships. The Carbis Bay communiqué also acknowledged the U.K.'s upcoming Future Tech Forum to examine emerging technology issues. The U.K.'s effort to expand R&D ecosystems includes new hiring and immigration schemes to attract international talent, as well as activities by the Royal Society to advance discussions about AI research and policy on an international level.

United States

Developments in the United States' AI governance began with the 2016 White House report, Preparing for the Future of Artificial Intelligence, which outlined the landscape of AI in the U.S., its current and potential applications, and the public policy implications of AI as an emerging technology that will affect operations and products across many sectors. In addition to identifying a need for review of regulations, the report also recognized a need to address the threat of unintended consequences by ensuring an ethical governance approach that emphasizes fairness and safety. The report addressed international cooperation, stating that the United States engaged on AI R&D in international forums including the U.N., the G-7, the OECD, and APEC, as well as on a bilateral basis with several countries, including most recently the EU in the newly formed U.S.-EU Trade and Technology Council. The report recommended that the United States government develop a government-wide strategy for international engagement on AI and "deepen its engagement" with international stakeholders in order to exchange information and facilitate collaboration.[103]

The White House simultaneously released its National Artificial Intelligence Research and Development Strategic Plan, which presents the United States' initial approach to investing in AI research and development, as well as the creation of a workforce prepared to lead AI R&D.[104] This 2016 strategic plan was updated in 2019 with the newest strategic priority stressing the importance of "effective partnerships between the federal government and

academia, industry, other non-federal entities, and international allies to generate technological breakthroughs in AI and to rapidly transition those breakthroughs into capabilities."[105] Also in 2019, Executive Order (EO) 13859 established the American AI Initiative with five guiding principles including that the United States "must promote an international environment that supports American AI research and innovation and opens markets for American AI industries."[106] Furthermore, EO 13859 declares that maintaining American leadership in AI necessitates "enhancing international and industry collaboration with foreign partners and allies."

With the enactment of the 2021 National Defense Authorization Act (NDAA), Congress authorized funding to create a National AI Initiative Office, AI Interagency Committee, AI Advisory Committee, and National Artificial Intelligence Research Resource Taskforce to spur research and development; promote technical skills training programs; convene federal agency leaders and public stakeholders; and issue recommendations on AI ethics and standards. The legislation also provides for a national research cloud to expand availability of computing power and datasets, among many other provisions to step up U.S. government engagement in AI.[107] Building on the principles in EO 13859 and agency-specific ethical frameworks of the Department of Defense, the Office of the Director of National Intelligence, and the Intelligence Community, Executive Order 13960 introduced additional principles to guide the trustworthy use of AI across U.S. government agencies.[108] In 2020, the Office of Management and Budget issued its Guidance for Regulation of Artificial Intelligence Applications to address risks and unacceptable harms in AI used by federal agencies; it explicitly rejected a precautionary approach, arguing that AI systems should not be held to an impossibly high standard that prevents society from enjoying the benefits of AI or undermining U.S. leadership in AI innovation and deployment.[109]

Under the Biden administration, focus on AI has continued to grow. Notably, this includes the launch of AI.gov and the formation of the congressionally-authorized National Artificial Intelligence (AI) Research Resource Task Force, which will be responsible for developing a national research infrastructure, including governance and ethical frameworks.[110] In addition, the Biden administration has initiated frameworks with the U.K., EU, and the U.K. and Australia together that include cooperation on AI.

Table 1. AI activities in the 7 administrations participating in the FCAI

	AI ethics Frameworks	Existing AI regulation	AI standards	Public Investment
Australia	Australia's AI Ethics Framework	Review of existing regulations per the AI Action Plan	Standards Australia focuses on by-design and standards testing; AI Standards Roadmap	AUD 124.1 million (USD 90.9 million) 2021-2022
Canada	CIFAR Pan-Canadian AI Strategy 2017; Digital Charter 2017/2021; Montreal Declaration for Responsible Development of AI	Directive on Automated Decision Making; Algorithmic Impact Assessment	CIO Strategy Council develops AI Standards and is accredited by Standards Council of Canada, focusing on ethical design and ADM audits; $8.6 million over five years, starting in 2021–22, to advance the development and adoption of AI standards	CAD 125 million (USD 100 million) 2017-2022
EU	Ethics Guidelines for Trustworthy AI; White Paper on AI; Proposal for a regulation on AI; National ethics guidelines	Coordinated Plan on AI; Proposal for a regulation on AI; Digital Decade package	CEN-CENELC Joint Technical Committee 21 'Artificial Intelligence'; national standards focus on EU interoperability, ethics, fundamental rights, and safety	EUR 20 billion (USD 23.3 billion) per year until 2030, national funding
Japan	R&D Guidelines 2018; Social Principles of Human-Centric AI 2019; AI Utilization Guidelines 2019; Society 5.0 framework	Draft AI Utilization Principles Guidelines 2019; AI Technology Strategy 2017	Ministry of Economy, Trade and Industry (METI), Japanese Industrial Standards Committee and Information Technology Standards Commission focus on developing sector-specific standards in transportation, safety, and patents	Yen 77 billion (USD 70 billion) 2018
Singapore	Model AI Governance Framework, 2nd Edition, 2020; Implementation and Self-Assessment Guide for Organizations; Principles to Promote Fairness, Ethics, Accountability and Transparency	National AI Strategy	Voluntary Horizontal Model Framework contributes to global standards for AI-related policies and guidelines	Up to SG$150 million (USD 110.8 million) 2017-2022
U.K.	Guidance on Ethics, Transparency Accountability for ADM	National AI Strategy	British Standard Institute (BSI) focuses on international cooperation and healthcare standards	GBP 1 billion (USD 1.36 billion) 2018-2027
U.S.	Principles in Executive Order 13859 and Executive Order 13960; Agency specific frameworks, state-specific guidelines	Government agencies assessing where AI regulation is needed, where existing regulation applies, and roles for self-assessment, codes, etc.	National Institute of Standards and Technology (NIST) and American National Standards Institute (ANSI) focus on maintaining U.S. leadership/ priority, international engagement, foundational AI standards	USD 1.9 billion 2018-2020

Note: Table 1 provides a non-exhaustive overview of FCAI governments' selected activities on ethics frameworks, existing regulations, standards bodies, and public investment figures for AI. Further data, explanation on the categories, and all references are listed in Annex 1. Conversion rate for public investment in local currency to USD from September 22, 2021.

In addition to the United States' participation in GPAI and several other international multistakeholder forums dedicated to cooperation on AI, recognition and commitment to international engagement on AI has been a consistent feature of U.S. policy across three administrations. The 2020 guidance explicitly mentions international regulatory cooperation, as defined in Executive Order 13609; it adds that "agencies should engage in dialogues to promote compatible regulatory approaches to AI and to promote American AI innovation while protecting privacy, civil rights, civil liberties, and American values;" as well as "consider existing international frameworks to which the United States has committed itself and the development of strategic plans for coordination and cooperation with international partners."[111] International cooperation was prominent in July 2021, when the National Security Commission on Artificial Intelligence hosted its Global Emerging Technology Summit focused on international cooperation, with speakers from NATO, the OECD, and the EU as well as several countries, and a total of five members of the Biden administration cabinet. U.S. Secretary of State Antony Blinken summed up U.S. policy by stating that cooperation on technology "is the most fundamental imperative of our time, and it extends beyond technology."[112]

2.2. AI cooperation in international bodies

The FCAI participants' domestic AI policies and engagement in international initiatives by FCAI participants as members of the G-7 and other multilateral initiatives provide a foundation for much broader international cooperation. This subsection provides an overview of the work of numerous international bodies working on AI. AI is also being discussed in national-security-focused forums such as NATO and the Organization for Security and Co-operation in Europe , but the national security dimensions of AI cooperation are beyond the scope of our work and are not explored here.

G-7

The G-7 (Canada, France, Germany, Italy, Japan, the U.K., the U.S., with the EU participating) has made cooperation on technology issues, including AI, a major focus. The 2017 G-7 ICT and Industry Ministers' Toronto Declaration headed its outcome declaration, "Making the Next Production Revolution Inclusive, Open and Secure."[113] In 2018, the G-7 specifically addressed AI in the Charlevoix Common Vision for the Future of AI,[114] committing to 12 general, human-centric AI principles. Following the 2018 G-7 Summit, Canada also hosted the G-7 Multistakeholder Conference on Artificial Intelligence with the theme of "Enabling the Responsible Adoption of AI," engaging over 200 experts, as well as representative stakeholder groups.[115]

Under the current U.K. presidency, the G-7 continues to play an important role in developing international coordination on AI; leading up to the 2021 G-7 summit, U.K. Health Secretary Matt Hancock signaled the U.K.'s intention to "look at internationally recognized standards" for ethical use of AI in healthcare and beyond. Furthermore, in March 2021, over 20 global companies released a statement urging the G-7 to "establish a new forum to discuss and agree on core principles that will guide their respective efforts to improve

governance of the digital economy," specifically mentioning AI.[116] The U.K.'s role is ongoing with its Future Tech Forum scheduled for late November as an occasion to discuss the role of technology in "open societies and [tackle] global challenges" in a collaborative multistakeholder forum.[117]

The U.K.'s role is ongoing with its Future Tech Forum scheduled for late November as an occasion to discuss the role of technology in "open societies and [tackle] global challenges" in a collaborative multistakeholder forum.

In addition to the body's continued engagement on artificial intelligence in their traditional forums for collaboration, the Global Partnership on AI (GPAI) can also be considered a G-7 spinoff, as it was developed and organized by France and Canada during their successive presidencies.[118]

Global Partnership for AI (GPAI)

The G-7 initiated GPAI in 2018. GPAI is a state-led multistakeholder initiative, now joined by 18 countries and the EU. It is perhaps the most comprehensive effort to date to establish a common understanding and approach to AI. GPAI has a Council and a Steering Committee, as well as working groups and committees, which are supported by a Secretariat hosted by the OECD and two "Centres of Expertise" based in Montreal (CEIMIA) and in Paris (INRIA). One key asset of this structure is a multidisciplinary network of policy, governance, and technical experts from academia, civil society, and industry. GPAI's mandate and scope of work has evolved toward practical solutions to "harness AI responsibly to solve pressing global challenges" in four working groups: Responsible Development, Use and Governance of AI, Data Governance, Innovation and Commercialization, and the Future of Work.[119] For 2022, the GPAI Council identified three key priorities: the fight against climate change; health and life sciences; and the impact of AI on human rights, gender equality, and inclusiveness.

G-20

The G-20 is made up of the 20 leading economies in the world, and includes China, Russia, and Saudi Arabia. It issued AI principles (based in turn on the OECD AI Principles) as part of its 2019 summit in Osaka and has continued to explore AI at subsequent summits. More recently, the Italian G-20 Presidency (2021) hosted a special event on AI and robotics.[120] At G-20 summits, invited group meetings alongside or ahead of the leaders' meetings also include discussions on AI, dubbed the B-20 (business), C-20 (civil society), L-20 (labor), S-20 (science), T-20 (think tanks), W-20 (women), and Y-20 (youth), as well as other forums for bringing together groups on focal issues in the G-20.

World Trade Organization (WTO) and trade agreements

Digital issues that can affect AI cooperation and development have played an increasingly prominent part in trade discussions. There are e-commerce negotiations underway in the WTO, which if successful could include a commitment to cross-border data flows that could support access to data for AI. Other trade agreements such as the U.S.-Mexico-Canada Agreement or the Comprehensive and the Progressive Agreement for Trans-Pacific Partnership also include commitments on AI-related data flows.[121] There are also AI-specific provisions in U.S.-Japan Digital Trade Agreement, the Digital Economy Partnership Agreement among Singapore, New Zealand, and Chile, and in the Australia-Singapore Digital Economy Agreement, among others.[122]

Organization for Economic Co-operation and Development (OECD)

The 37-member OECD explored cooperation in AI as early as 2016. An AI Group of Experts then developed Principles on AI in 2018, which were adopted by member countries in May 2019 as the OECD Council Recommendations on Artificial Intelligence. These are not legally binding but have been influential in shaping international discussion regarding AI practices and standards and the design of national legislation on AI. The OECD Network of Experts on AI (ONE AI) and the launch of the OECD.AI Policy Observatory (OECD.AI) also shape the international debate on AI governance and policy while supporting the OECD's function as the secretariat for GPAI. In addition, the OECD hosts a multistakeholder expert group which includes 100-150 representatives from think tanks, business, civil society and labor associations, and other international organizations. The group contributes to developing principles for competitive, trustworthy, and internationally inclusive AI development considering the transformative impact of AI on society, economy, and policy. The plenary of the OECD multistakeholder expert group develops annual reports and recommendations based on applied AI project work which takes place in the working groups.

The OECD plays a significant role in international cooperation both through its recommendations and in its capacity as the GPAI secretariat. To monitor implementation of the OECD AI principles, it has convened representatives and experts from numerous countries, including outside the OECD. In June 2021, it issued a report, The State of Implementation of the OECD AI Principles, which describes national and multilateral policy development, makes general recommendations for AI policy development, and reports on international cooperation.[123] The OECD, in partnership with several multilateral organizations, has extended its observatory function by establishing an online portal on international cooperation with links to the organizations involved and activities grouped under the headings of trustworthy and ethical AI, human rights and democracy, and advancing the SDGs.[124]

United Nations (U.N.)

The U.N. has several AI-related strands of work in its respective agencies. The International Telecommunications Union (ITU) hosts an annual "AI for Good Global Summit," engaging 37 U.N. partners to apply AI technologies toward advancing the SDGs. Other U.N. agencies work on diverse issues such as the International Labor Organization's research on AI and jobs or the Human Rights Council's proposed resolutions on new and emerging digital technologies and human rights.[125] UNESCO has been working on its own comprehensive recommendations on ethics for AI and hopes to adopt a final instrument aimed at use cases and concrete measures at the UNESCO General Conference late in 2021.[126] The Secretary General's Roadmap for Digital Cooperation identifies several key issues: a lack of inclusiveness in AI global discussions; inadequate overall global AI cooperation; and few easily-accessible AI initiatives for countries outside established groupings.[127] The U.N.'s 17 SDGs adopted in 2015 have been key reference points for most of the multilateral discussions mentioned above on deploying AI for social good.

Council of Europe (CoE)

The CoE is the first international organization (excluding the EU) to examine possible adoption of internationally-binding rules for AI. The Committee of Ministers established an Ad Hoc Committee on Artificial Intelligence (CAHAI) in 2019, which is examining the feasibility and potential elements of an international legal framework on AI to protect human rights, democracy, and the rule of law that substantially follows the EU's risk-based approach.[128] CAHAI's multistakeholder membership is composed of representatives from the CoE's 47 member states, observer state representatives (including Canada, Holy See, Israel, Japan, Mexico, and the U.S.), other international and regional organizations (including the EU, U.N., OECD, and OSCE), and the private sector, civil society, research, and academic institutions. CAHAI published a feasibility study in 2020 with nine key principles and potential substantive rights and resulting obligations;[129] it also assessed the roles and responsibilities of states and private actors in compliance, liability, and safety questions.[130] At this stage, it remains to be seen which AI definition the CAHAI agrees on, and which regulatory elements will be adopted by the CoE Council of Ministers.

Asia Pacific Economic Cooperation (APEC)

APEC, whose member states include Singapore, Australia, Japan and the US, convenes work on AI mainly in its Digital Economy Steering Group.[131] In 2020, the APEC Business Council published an overview report with specific AI use cases in each APEC member country, as well as a summary of their respective AI strategies, institutional agencies, and notable AI or data initiatives. [132] The report promotes "elevating AI in APEC's economic agenda" and lists six policy recommendations to support the trustworthy, innovation-friendly, and regulatory coherent uptake of AI in APEC member states.

Other bilateral and multilateral agreements

EU-Japan, France-Canada, United States-United Kingdom, Singapore-Australia, and Germany-India are examples of countries that have or are in the process of concluding bilateral agreements or memoranda of understanding on various matters for cooperation on AI.[133] Likewise, five nations—Estonia, South Korea, Israel, New Zealand, and the U.K.—formed the D5, a group that self-identifies as "some of the most digitally advanced governments in the world," convening a thematic group on AI in its annual meeting.[134] The U.S., Australia, Japan, and India have formed The Quad" to cooperate in development of artificial intelligence along with quantum computing to avoid Chinese dominance in these fields. The U.S. has also spearheaded governmental cooperation networks by bringing together seven EU member states, Australia, Canada, and South Korea, "to provide values-based global leadership in defense for policies and approaches in adopting AI."[135]

2.3. International AI cooperation through standards development organizations (SDOs)

Leaders, including those from all FCAI participant governments, have endorsed the key role of multistakeholder industry-led standards bodies in developing AI standards. A defining feature of these standard-setting bodies is that they are transnational private bodies. Governments do participate in their processes but historically only as participants in industry-led efforts. This reflects the emphasis of these bodies on standards processes that are technical and expert-driven.[136]

The 2021 G-7 leaders' communiqué included various commitments of support for "industry-led inclusive multi-stakeholder approaches to standard setting" and endorsed the Framework for G-7 Collaboration on Digital Technical Standards, a set of steps the G-7 will take to strengthen international cooperation with respect to digital technical standards.[137] This followed a call to action by heads of G-20 standards organizations, along with the International Electrotechnical Commission (IEC), International Organization for Standardization (ISO) and International Telecommunication Union (ITU), to "recognize, support and adopt international standards to accelerate digital transformation in all sectors of the economy.[138] The 2019 OECD AI Principles also includes recognition of a need to "promote the development of multi-stakeholder, consensus-driven global technical standards for interoperable and trustworthy AI.[139] The Technical Barriers to Trade Committee of the WTO in 2000 recommended six principles to guide preparation of international standards, namely transparency, openness, impartiality and consensus, effectiveness and relevance, coherence, and addressing the concerns of developing countries.[140]

The ISO, IEC, and IEEE are the key multistakeholder industry led SDOs for developing international voluntary consensus AI standards and have been the focus of our AI Dialogues. While the ITU's Telecommunication Standardization Sector (ITU-T) is also multistakeholder and inclusive of industry, it appears to lack credibility when it comes to developing AI standards, in part due to perceived Chinese influence that has raised concerns that the ITU-T cannot be a "neutral arbiter."[141]

Both the ISO/IEC and IEEE are undertaking significant work on AI standards. For example, the ISO/IEC established JTC 1/SC 42 to develop AI standards in 2017, and is currently developing the terminology and definitions relative to AI technologies, as well as standards for interoperable frameworks for AI systems, risk assessment, algorithmic bias, AI lifecycle, and AI trustworthiness. The IEEE is addressing the intersection of technology and ethical considerations for AI, including work on algorithmic bias and a model process for addressing ethical concerns during system design.[142]

A defining feature of these standard-setting bodies is that they are transnational private bodies. Governments do participate in their processes but historically only as participants in industry-led efforts. This reflects the emphasis of these bodies on standards processes that are technical and expert-driven.

SDOs have different representation and operating procedures. The table in Annex 1 (page 92) provides an overview of the membership and voting procedures of the ISO, IEC, IEEE and ITU-T. The international standards they develop are consensus-based and voluntary, in that it remains up to governments and businesses whether to use them. Nevertheless, they can have a very significant influence both at the domestic level and for international trade. For example, previous ISO/IEC standards have a history of being adopted by companies globally, becoming de facto standard for market access. In addition, governments increasingly reference ISO/IEC international standards in domestic laws or regulations.[143] International standards can also be enforced via contract and as a basis for industry self-regulation.

2.4. Non-governmental cooperation on AI

Alongside and outside the various institutions discussed above, there are many intersecting networks of industry, civil society, and academics that provide robust and diverse avenues of cooperation and bring informed, practical, and diverse voices to all aspects of AI development and its economic and social impact. Most multilateral initiatives, such as the G-20, also include nongovernmental organizations, businesses, academia and think tanks, advocacy groups, and other civil society and experts.[144] The European Commission established the High-Level Expert Group for AI (AI HLEG) in 2018. Comprised of 52 experts (23 corporate, 19 academic, and 10 civil society representatives), the HLEG-developed Ethics Guidelines for Trustworthy Artificial Intelligence,[145] Policy and Investment Recommendations for Trustworthy AI[146] and the Assessment List for Trustworthy Artificial Intelligence[147] that provided important reference points for the European Commission in developing its AI strategy and regulatory proposal on AI. The AI HLEG continues to act as the steering group for the European AI Alliance, a broader multistakeholder forum with over 4,000 international members.[148]

Many organizations have convened discussions of AI cooperation too numerous to catalog here. Examples include:

- The World Economic Forum (WEF) brings together government officials, businesses, and civil society and has launched a Global AI Action Alliance advancing international cooperation on AI with partnering organizations.[149]

- The Open Community for Ethics in Autonomous and Intelligent Systems (OCEANIS) is a global forum for discussion, debate and collaboration amongst organizations interested in development and use of standards to further the development of autonomous and intelligent systems.[150]

- The AI Now Institute based at New York University has published annual reports and hosted conferences on specific AI-related issues,[151] which have received international attention on its research related to societal issues including equality, safety, and human rights.

- European civil society organizations like European Digital Rights (EDRi), Access Now, or the European Consumer Organisation (BEUC) undertake similar work on consumer rights with a specific, more recent focus on scrutinizing facial and emotion recognition systems.
- In addition, there is an array of think tanks that are focused on AI issues in addition to Brookings and CEPS. Private initiatives like the Partnership on AI, established by Apple, Amazon, DeepMind, Google, Facebook, IBM, and Microsoft, contribute to the international discussion on AI.

2.5. Conclusion: Mapping the space for international collaboration

The avenues of cooperation on AI described above demonstrate rich interest in AI and AI cooperation across multiple governments, sectors, and channels. These provide strong centripetal forces to harness effective and productive cooperation. Nevertheless, there remain strong centrifugal forces that may impede cooperation. Perceptions of national interests through a lens of mercantilism see cooperation as a threat to development of national industries. Differences in systems of government and law as well as culture can lead to different approaches to regulation and risk or difficulty in understanding other approaches. Despite shared commitments to human rights and democratic values, there are differences in how these are appreciated.

These forces mean that complete convergence or alignment of policies and rules on AI among FCAI participants or likeminded countries is unlikely. But significant convergence and alignment are conceivable in various areas and to various extents. Section 3 explores concrete ways to build on the wide interest in international cooperation.

The avenues of cooperation on AI demonstrate rich interest in AI and AI cooperation across multiple governments, sectors, and channels. These provide strong centripetal forces to harness effective and productive cooperation.

3.

RULES, STANDARDS, AND R&D PROJECTS: KEY AREAS FOR COLLABORATION

Our exploration of international AI governance, based on eight FCAI roundtables and several bilateral discussions with participants, led us to identify three main areas where enhanced collaboration would prove fruitful: regulatory policies for AI, standard-setting, and R&D projects. Below, we analyze the way in which cooperation may unfold in each of those areas, as well as the extent of collaboration that can be envisaged in the short-term as well as longer-term.

3.1. Cooperation on regulatory policy

International regulatory cooperation, as discussed in Section 1, has the potential to reduce regulatory burdens and barriers to trade, incentivize AI development and use, and increase market competition at the global level. That said, countries differ in legal tradition, economic structure, comparative advantage in AI, weighing of civil and fundamental rights, and balance between ex ante regulation and ex post enforcement and litigation systems. Such differences will make it difficult to achieve complete regulatory convergence. Indeed, the national strategies and policies outlined in Section 2.1 (page 27) reflect differences in countries' willingness to move towards a comprehensive regulatory framework for AI: The European Commission has already taken a step in that direction, whereas others at least initially have opted for a more self-regulatory approach (e.g., Singapore). Likewise, at first sight there are differences among jurisdictions willing to adopt horizontal rules applicable to all sectors of the economy (the EU), and countries that have begun with a more sectoral focus (the U.S.).

Despite these differences, there has been significant convergence on key principles for responsible AI development, especially among democratic countries, that provides a common basis for AI regulation. Moreover, as AI policy development is in the relatively early stages in all countries, alignment of AI policies and regulations is easier to achieve now than later, when policies become already fully shaped and enacted in each country.

As noted, among the seven participating FCAI governments, Australia, the EU, Japan, and Singapore have developed comprehensive sets of principles for the responsible development of AI. The OECD has echoed these (in particular, the EU ones) by developing a list that expands the scope of responsible AI development toward a multistakeholder approach, as well as postulating a need for governments to develop safeguards to promote responsible development and deployment of AI. Table 2 below shows a useful comparison chart presented by BSA/the Software Alliance that illustrates the ongoing convergence among these principles.[152] As mentioned in the introductory section, where this convergence of AI principles leads in terms of AI regulation remains to be seen.

Table 2. International frameworks for the development of responsible AI

Values	Definitions	EU	Australia	Japan	Singapore	OECD
Human centered	AI systems should be designed to be inclusive, accommodating the needs of the individuals that interact with it, and used in a manner that is aligned with the values of the community in which it is deployed.	✓	✓	✓	✓	✓
Mitigate risks and promote benefits	AI systems should be designed and deployed for the benefit of end users and avoid unintended negative impacts on third parties.	✓	✓	✓	✓	✓
Fairness	Governance and technical safeguards are important to identify and mitigate risks of unfair biases, particularly in circumstances where an AI system could have a consequential impact on people.	✓	✓	✓	✓	✓
Explainability	AI systems should be understandable; context will dictate the appropriate mechanisms for providing transparency about a particular system's decisionmaking processes.	✓	✓	✓	✓	✓
Privacy and security	AI systems should be secure and enable users to make informed choices regarding use of personal information.	✓	◑	✓	○	✓
Safety and reliability	AI systems should be designed to mitigate foreseeable safety risks and adequately tested to ensure that they operate as intended.	✓	✓	◑	✓	✓
Accountability	A lifecycle approach to AI accountability, including appropriate governance structures for the design phase and redress mechanisms following deployment is important.	✓	✓	◑	✓	✓
Risk-based and proportionate	Risks are context-specific and encourage stakeholders to deploy risk management techniques that are tailored to specific use cases.	✓	✓	○	✓	✓
Multiple stakeholders	Multiple stakeholders have important roles to play in mitigating risks involved in the development, deployment, and use of AI.	◑	◑	✓	✓	✓
Promotes innovation	Government is a key enabler of AI innovation, and promotes a policy environment that is conducive to cross-border data flows, value-added data services, access to non-sensitive government data, R&D, and workforce development initiatives.	○	◑	✓	○	✓

✓ **Satisfactory** ◑ **Partial** ○ **Unaddressed**

Source: BSA/The Software Alliance[153]

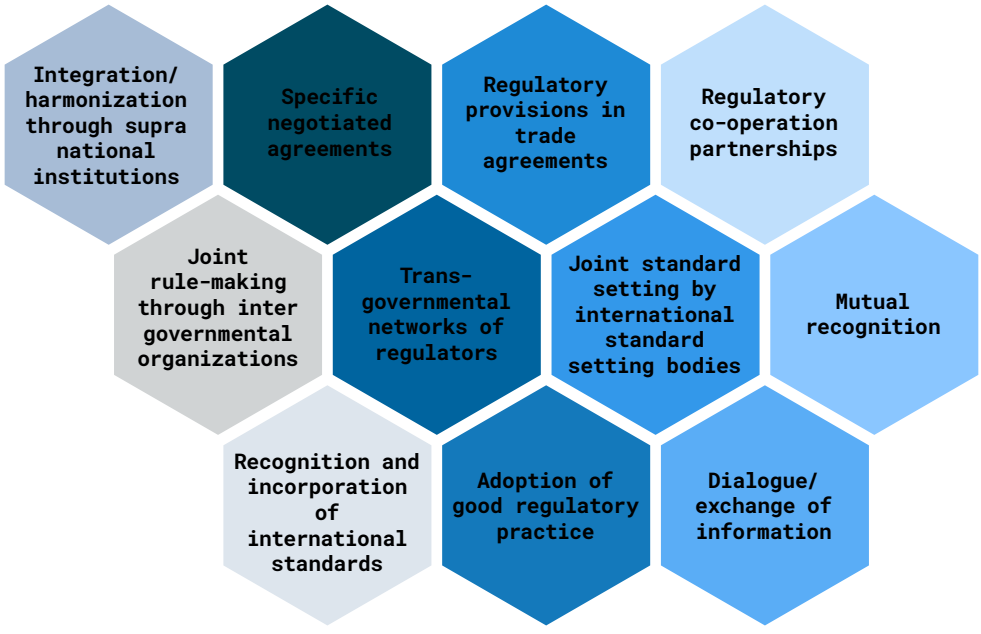
In the ever-changing environment of AI development and innovation, agreeing on conceptual approaches that will guide the scope of both regulatory and non-regulatory requirements can provide a starting point for international convergence in AI policy and development. At the same time, alignment on principles is only a first step in such collaboration. While agreeing on common principles of ethical or trustworthy AI may be relatively easy for the seven administrations involved, the degree of agreement as to how these principles should be effectuated in regulatory approaches and frameworks is likely to prove more challenging. It is on the effectuation of common principles that we focus this discussion.

Agreeing on conceptual approaches [to AI development and innovation] that will guide the scope of both regulatory and non-regulatory requirements can provide a starting point for international convergence in AI policy and development.

When it comes to international regulatory cooperation (IRC), several mechanisms are possible. One possible reference, shown in Figure 2, is the OECD taxonomy of IRC mechanisms, which range from very light exchanges such as FCAI (dialogue/exchange of information) to more substantial forms of cooperation such as exchange of good practices, incorporation of international standards or joint standard setting, mutual recognition, ad hoc regulatory provisions in trade agreements, and even complete harmonization through supranational institutions.

Against this backdrop, AI presents an opportunity for IRC to achieve significant integration because it is less linked to pre-existing legal traditions or frameworks. Below, we identify a number of areas in which cooperation would be fruitful, and we discuss the extent to which it can be expected given existing initiatives and the experiences and interests in the seven administrations that participate in FCAI. The areas for cooperation identified below, as well as our assessment of the mode and extent of cooperation we consider attainable, are informed by the FCAI dialogues and discussions with individual participants.

Figure 2. OECD mechanisms of international regulatory cooperation



Source: International Regulatory Cooperation, Addressing Global Challenges, OECD (2013).

3.1.1. A common, technology-neutral definition of AI for regulatory purposes

Adopting a common definition of AI would provide an important building block for international regulatory cooperation. Policymakers face important challenges when it comes to adopting an operative definition of artificial intelligence. A relatively narrow definition may lead to more targeted regulatory efforts, especially where specific AI techniques (e.g., machine learning) are the ones that create the greatest concerns for regulators. At the same time, the narrower the definition, and the more it is related to a particular method, the less technology-neutral and future-proof the definition is likely to be. The emerging tendency to blend different AI techniques in the same system also makes any narrow definition difficult to justify and implement as well as easier to game.[154]

The current landscape of definitions of AI among FCAI participants is already becoming heterogeneous, as shown in Table 3 below. Several official definitions have been adopted as part of general policies rather than aimed more specifically at regulatory purposes. Only the definition proposed in the EU's draft regulation—and adopted in U.S. appropriations legislation and incorporated into the U.S. Office of Management and Budget (OMB) guidelines—appear to fit the latter purpose. Table 3 summarizes the existing definitions in the seven governments participating in the FCAI.

At the international level, a subgroup of the OECD AI network of AI experts has done useful work to harmonize a workable comprehensive proposal. The resulting definition reads as follows:

> *"An AI system is a machine-based system that can, for a given set of human-defined objectives, make predictions, recommendations or decisions influencing real or virtual environments. It does so by using machine and/or human-based inputs to: i) perceive real and/or virtual environments; ii) abstract such perceptions into models through analysis in an automated manner (e.g., with ML, or manually); and iii) use model inference to formulate options for information or action. AI systems are designed to operate with varying levels of autonomy."*[155]

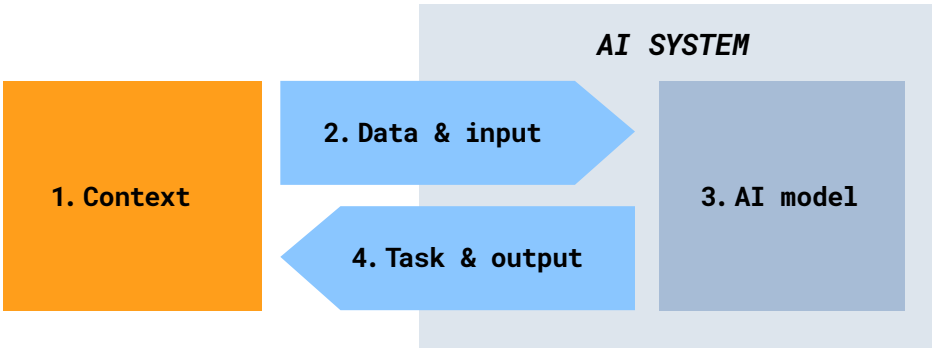
Table 3. AI definitions in the 7 administrations participating in the FCAI

Country	Definition
Australia: AI Action Plan	"A collection of interrelated technologies that can be used to solve problems autonomously and perform tasks to achieve defined objectives." "[In some cases, AI] can do this without explicit guidance from a human being …"[156] "AI is more than just the mathematical algorithms that enable a computer to learn from text, images or sounds. It is the ability for a computational system to sense its environment, learn, predict and take independent action to control virtual or physical infrastructure."[157]
Canada: Directive on Automated Decision-Making	"Information technology that performs tasks that would ordinarily require biological brainpower to accomplish, such as making sense of spoken language, learning behaviours, or solving problems."
European Union: AI White Paper and AI Act	"Software that is developed with one or more of the techniques and approaches listed in Annex I and can, for a given set of human-defined objectives, generate outputs such as content, predictions, recommendations, or decisions influencing the environments they interact with."
Japan: Contract Guidelines on Utilization of AI and Data	"A generic term for a series of software technologies that enable computers to perform intellectual activities that can be performed by humans." The Guidelines assume the term "AI technology" to mean either "machine learning" or a "series of software technologies related to machine learning". The terms "machine learning," "supervised learning," "unsupervised learning," and "deep learning" are also defined (METI, 2019).[158,159]
Singapore: Model AI Governance Framework	"A set of technologies that seek to simulate human traits such as knowledge, reasoning, problem solving, perception, learning and planning, and, depending on the AI model, produce an output or decision (such as a prediction, recommendation, and/or classification)." This definition is specifically formulated for the purposes of this framework.[160]
United Kingdom OAI (2019) 'A guide to using artificial intelligence in the public sector'	AI can be defined as "the use of digital technology to create systems capable of performing tasks commonly thought to require intelligence. AI is constantly evolving, but generally it: Involves machines using statistics to find patterns in large amounts of data. Is the ability to perform repetitive tasks with data without the need for constant human guidance."[161]
United States: Section 238(g) of the FY2019 National Defense Authorization Act	"Any artificial system that performs tasks under varying and unpredictable circumstances without significant human oversight, or that can learn from experience and improve performance when exposed to datasets. "An artificial system developed in computer software, physical hardware, or another context that solves tasks requiring human-like perception, cognition, planning, learning, communication, or physical action. "An artificial system designed to think or act like a human, including cognitive architectures and neural networks. "A set of techniques, including machine learning, that is designed to approximate a cognitive task. "An artificial system designed to act rationally, including an intelligent software agent or embodied robot that achieves goals using perception, planning, reasoning, learning, communicating, decision-making, and acting."

The OECD group also developed a classification of AI systems divided into four dimensions:

- Context (the environment where the system is being deployed and who is deploying it).
- Data and input (the data the system uses and the kinds of input it receives).
- The type of AI model (the underlying design and operation of the AI system—is it, for instance, a neural network or a linear model).
- The tasks the system performs and the outputs that are the product of its work.[162]

Figure 3. The OECD AI system model



Source: OECD AI Policy Observatory (2021).

The OECD definition has already triggered some degree of convergence. For example, the EU AI Act proposes a definition that is largely in line with the OECD's (see Table 3). Ensuring that all countries involved in the FCAI have a voice in defining the term and updating it would help ensure the compatibility of national legislation, enabling smoother international cooperation. For this reason, we hosted a discussion on definitions of AI in our FCAI dialogues. Moreover, insofar as countries converge on a risk-based approach to AI regulation (see below), it is important that the definition of AI adopted at national and international levels is technology-neutral and broad.

3.1.2. Building on a risk-based approach to AI regulation

The approach by which regulatory effort should be proportionate to risk generated by a given AI application appears to be endorsed explicitly by most governments participating in FCAI. Both in national strategies and in bilateral or multilateral contexts, a risk-based approach has been endorsed by a variety of different bodies: from the U.S.-Japan Business Council,[163] to the Council of Europe, to several stakeholders from industry and civil society.

A risk-based approach is central to the policy frameworks of the two most prominent exemplars of AI policy development—the U.S. and the EU.

Most notably, a risk-based approach is central to the policy frameworks of the two most prominent exemplars of AI policy development—the U.S. and the EU. In the EU, the proposed AI Act is consistent with and builds on experience regulating other risks to human health. Its assessment of risks includes not only risks of AI to human safety and security (addressed

by enlarging the application of existing EU regulation) but also risks to EU fundamental rights. The EU AI Act's risk-based approach to sectors and applications means that it is targeted rather than broadly applied to all forms and uses of AI. In the United States, the OMB ten principles include risk assessment and management, in the belief that "it is not necessary to mitigate every foreseeable risk … Instead, a risk-based approach should be used to determine which risks are acceptable and which risks present the possibility of unacceptable harm, or harm that has expected costs greater than expected benefits."[164] The U.S. National Institute of Standards and Technology (NIST) is developing an "Artificial Intelligence Risk Management Framework"); this framework will provide voluntary guidance to assess and improve the trustworthiness of AI products, services, and systems, drawing on standards, best practices, and other references.[165]

These recent, broadly parallel developments have opened the door to developing international cooperation on how to address risks while maximizing benefits. Annex III to the EU's proposed legislation lays out a detailed series of steps and practices for assessment and accountability; the NIST AI risk management framework will distill broad input and source material into an adaptable and implementable framework. Both inform further exploration of risk assessment and risk management in the context of AI.

Despite this initial consensus on the merits of a risk-based approach, there remain challenges converging on a risk-based approach to AI, for several reasons. The FCAI has discussed the issue of convergence on risk regulation at some length, and the following issues have emerged as candidates for exploring enhanced international cooperation:

- **What are the risks?** Depending on the use case, AI can generate risks for any fundamental and human rights as well as for safety and security.[166] At the same time, various national strategies appear to focus on different sets of possible risks.[167] Still, the potential safety and security risks generated by AI appears to be under-researched, despite recent important contributions in this specific domain. Beyond these risks are more collective risks generated by AI systems, which may fall outside existing approaches to risk assessment. These encompass systemic risks, including risks associated with major events such as the collapse of critical infrastructure; risks to the democratic process, and epistemic risks generated by the increasing use of partly explainable AI techniques especially in scientific fields. These risks may derive more broadly from technology, networks, and information and not just AI as such. Nevertheless, their interaction with AI systems warrants consideration. In addition, interactive risks are likely to become increasingly prevalent as learning-based AI systems pervade the economy, potentially leading to inadvertent and unintentional impacts due to the interaction between different algorithms operating in the same environment. Discussing these risks at the international level (including in the FCAI) and sharing practices in monitoring and mitigating them would be extremely important for the future of AI policy cooperation.

- **What approach to benefit-risk analysis?** As discussed in two FCAI dialogues on AI risks, even with agreement on a risk-based approach, countries may end up differing in how they weigh the benefits and risks associated with the use of AI, and also may differ in how or whether they consider risks and benefits if AI is not used. These differences will require additional discussions on how the risk associated with specific AI applications should be assessed against the prospective benefits; whether AI risks and benefits should be compared against the status quo; and how to take account of AI that mitigates risks that would occur without its use. One could imagine situations arising in which not using well-established, safe AI to address a specific problem could fall short of standards of responsible conduct. Comparing approaches across FCAI governments and other organizations will be useful and important.

- **How are the risks classified?** Building a risk-based approach implies that riskier AI systems can be distinguished from less risky ones, so that possible mitigating measures can apply accordingly. In the European Union, the AI Act proposes a four-level risk classification system: with certain AI systems considered to generate unacceptable risks; others classified as high-risk; a smaller and more specific group labeled as moderately risky; and the rest considered as low risk. This classification, which marks a shift from the original binary proposal (high-risk or low-risk) presented by the European Commission in its 2020 AI white paper, also responds to some of the criticisms advanced by academics and stakeholders during the open public consultation and comes closer to the five-level approach proposed by the German Data Ethics Commission.[168] This risk classification also echoes, to some extent, the approach adopted in specific policy domains (e.g., medical devices)[169] and provides a model for international discussion of risk classification and exchange of practices. The NIST AI Risk Management Framework is developing another model. It aims to be "adaptable" and "scalable" to organizations of all sizes and types as well as AI across technologies, sectors, applications, and lifecycles.[170]

  Convergence on the risks posed by AI systems could lead toward consistent risk assessment and risk management for AI applications in different countries. This, in turn, can underpin regulatory cooperation. This would also help increase understanding of the potential mitigating measures that may ease the specific concerns raised by individual AI applications over time. A key benefit of international cooperation in this respect would be the potential to keep up with the rapid development of technology by continuously updating and benchmarking AI applications by sector and use case. Such tracking could operate by maintaining a matrix of the related classification systems in different countries, perhaps encompassing a register for AI applications associated with various risk levels. The availability of such information could help to identify differences and enable these to be reduced through cooperation and dialogue. Convergence in risk classification systems would reduce adjustment costs for those AI developers and deployers that wish to serve global markets and can thereby enhance consumer choice. Even in the absence of convergence, the availability of consistent global risk

classification information could help AI developers direct their efforts and adjust their governance, technical, and organizational arrangements when developing or deploying AI solutions

- **Are there cases in which the risks are too high to be mitigated?** Agreement on risk classification may also imply convergence on uses of AI that present risks that are difficult—or even impossible—to mitigate.[171] These uses may also be directly related to cases where protection of the democratic process, safeguards for fundamental rights, and significant, or even catastrophic, safety and security risks warrant a moratorium on the deployment of specific types of AI solutions. For example, the EU AI Act proposes to classify as unacceptably risky specific AI systems that manipulate human behavior to circumvent users' free will (e.g., toys using voice assistance that encourage dangerous behavior of minors); systems that allow "social scoring" by governments; and certain remote biometric identification in public places. The latter has been the subject of wide public concern from data protection authorities in Europe and various states and municipalities in the U.S.

  While the specific descriptions probably need further clarifications (e.g., various consumer-facing AI applications manipulate human behavior to different extents without being necessarily worthy of a ban), there appears to be scope for FCAI governments to explore AI systems that may pose risks so high that they should be banned outright or subject to a moratorium pending further study.

- **What is the type of risk assessment, and who performs it?** Once the boundaries of AI risk are established (whether by law or otherwise), key decisions relate to how assessment of a particular system or application should be performed, as well as who should perform the assessment. Agreement on a risk taxonomy may facilitate convergence in this domain.[172] Several auditing frameworks for AI systems are emerging in international standardization bodies and other organizations, as described in Section 3.1.3 below, that may inform these choices and establish a basis for this assessment.[173] Who performs an assessment is likely to be shaped by the nature of the assessment and by law or regulation like frameworks for a third-party conformity assessment. Some assessments could be performed in-house by AI developers, who are more likely to be aware of internal design features of the algorithm; or by deployers, who are often better positioned to gauge the risk associated with the individual use case and arrange mitigating measures such as human oversight or transparency.

  The content of risk assessments for specific systems or uses brings together all the factors that define whether specific AI can be considered safe or trustworthy. These include principles or requirements for responsible AI, risks and benefits, and regulatory models for AI. Accordingly, future cooperation among governments participating in FCAI depends on the extent of the alignment of AI principles and risk-benefit analysis with the ways that these approaches are put into practice. Cooperation will require thorough ongoing exchange on specific risk mitigation measures or processes (e.g., on what constitutes

meaningful human oversight); on how to audit AI to avoid bias and discrimination; on what explainability means, for whom, and in what context; on what constitutes high-quality data, whether and how training data should be stored, and how to deal with cases in which keeping the data is more challenging; on when and how to comply with transparency requirements; and on how to scale or adapt these measures and processes to different risk levels, uses cases, scales of operation, or types of organizations.

- **What happens after deployment?** Risks can be detected before an AI system reaches the market, but can (and are very likely to) emerge afterward, especially when the AI system is designed to learn over time. Against this backdrop, it is important that emphasis on ex ante risk assessment is accompanied by risk management throughout the life of the AI system. This may imply additional practices, such as repeating the risk assessment periodically; monitoring of the AI system's performance and behavior; and setting up redress procedures, including the swift remote update of the AI system, or its withdrawal from the market where the risk warrants it and no immediate mitigating measures are available.

On all these questions cooperation is possible and desirable. The approaches to risk regulation vary on the two sides of the Atlantic, although the traditional view that the EU is always more precautionary than the U.S. has scant support in the empirical evidence.[174] Even so, differences in the approach to promotion of trustworthy AI might emerge between the European Commission's proposed risk classification system, focused on risks for fundamental rights and safety, and the U.S. case-based regulatory approach, directed to maximize net benefits from using AI (potential economic, environmental, public health and safety, and other advantages; distributive impacts; and equity).

Moreover, the announced U.S. approach to AI risk assessment (OMB 2020 and Executive Order No 13563 / 12866 and the NIST AI RMF) is evolving and not yet fixed in one law as the EU contemplates.[175] Compared to the proposed EU AI Act, the U.S. approach relies to a greater extent on non-regulatory approaches, especially in sectors or use cases where existing regulations are deemed sufficient or when the benefit of a new regulation would not justify its costs. And when it comes to the post-market phase, differences may emerge on the obligations related to post-deployment surveillance, as well as on the liability regime that will be applied to AI, on which the European Commission is expected to adopt an initiative. A clear understanding of the degree and similarity and differences can help to minimize unnecessary divergence.

3.1.3. Sharing experiences and developing common criteria and standards for auditing AI systems

Independent of the extent or nature of the regulatory framework adopted in different countries, there will be significant scope for algorithmic auditing practices, both ex ante as well as following deployment of AI systems. The EU's proposed AI regulation includes both. It brings to bear existing EU product safety legislation on all high-risk AI systems that are embedded in products already covered by this body of law, requiring third-party conformity assessment for these uses as well as remote biometric identification. For all

other high-risk uses, the proposed regulation leaves conformity assessments to "internal control checks" by the AI providers.[176] While the proposed text in the body of the regulation is not very prescriptive when it comes to the description of the conformity assessment procedure or the quality management system to ensure compliance, Annexes IV and VII of the regulation spell out the documentation required and outline specific steps that will need to be taken. Even where independent third-party auditing is not required, a likely outgrowth of the AI Act will be to pave the way for emergence of an international market for AI auditing standards.[177]

The field of accountability in AI and algorithms has been the subject of wide and valuable work by civil society organizations as well as governments:

- The U.S. Government Accountability Office recently published an "Accountability Framework for Federal Agencies and Other Entities," which emphasizes the need for constant oversight and monitoring to ensure the reliability and relevance of AI systems throughout their life cycle.[178]

- Singapore's model AI governance framework contains guidance on internal governance structures and measures as well as on choosing an AI decisionmaking model.[179]

- The Japanese Society for Artificial Intelligence adopted principles of AI design to ensure that AI R&D remains beneficial to human society, and that development and research is conducted ethically and morally. The recent EU-Japan bilateral exchange on AI also emphasized possible techniques to preserve the accuracy and reliability of AI systems both ex ante and during their operations.[180]

- The EU High Level Expert Group provided guidance on how to carry out self-assessment of AI's trustworthiness by releasing the Assessment List on Trustworthy AI in June 2020.[181]

- The IEEE has developed standards for ethically aligned design over several years, leading to a publication in 2019.[182]

- In a study for the German Federal Office for Information Security, Berghoff et al. provide an in-depth overview of the auditing process for different types of AI—focused mainly on the security aspects.[183]

- The U.K. Information Commissioner's Office published its Guidance on the AI Auditing Framework. It covers best practices for compliance with data protection laws in development and deployment of AI systems and focuses on accountability and governance; data protection impact assessment; lawfulness, fairness, and transparency; security and data minimization; and individual rights in AI systems.[184]

- The Partnership on AI hosted important discussions for the development of an end-to-end approach to internal algorithmic auditing, including an analysis of how to learn across industries.[185]

- At the sectoral level, work on algorithmic auditing is intensifying with several sector-specific frameworks being developed in finance, health care, and intelligence. One recent example is the World Health Organization's "Guidance on ethics and governance of artificial intelligence for health."[186]

- The GPAI working group on responsible AI has proposed development of a common assessment framework, which could become the basis for further alignment and dialogue among the participating institutions.[187]

The work of international standardization bodies such as IEEE and ISO/IEC is especially important in the development of auditing standards. It will provide important reference points to stimulate uptake and recognition of good practices in AI development and deployment, both for auditing practices and for any prescriptions by government. A number of questions arise that deserve additional reflection to develop more agile and dynamic frameworks for auditing AI. For example, the scope of AI auditing may change significantly depending on the sector and use case, and whether auditing is done at the development stage or deployment stage, or is or focused on specific risks (e.g., fundamental rights or safety). Moreover, enhanced cooperation on principles for government AI procurement could also become a catalyst for meaningful development and convergence in the auditing of AI systems (see below, Section 3.1.6.).[188]

The exchange of good practices and ultimately a common—or at least a compatible—framework for AI auditing would eliminate significant barriers to the development of a truly international market for AI solutions. It also would facilitate the emergence of third-party auditing standards and an international market for AI auditing, with potential benefits in terms of quality, price, and access for auditing services for deployers of AI. Additionally, the development of the exchange of practices and international standards for AI auditing, monitoring, and oversight would significantly help the policy community keep up to speed in market monitoring.

The exchange of good practices and ultimately a common—or at least a compatible—framework for AI auditing would eliminate significant barriers to the development of a truly international market for AI solutions.

Where governments adopt regulatory schemes (whether broadly applicable as the EU's proposed regulation would be, or along sectoral lines), cooperation among enforcement bodies will become important, especially when it comes to the application of rules with extra-territorial effects (as is the case, e.g., for the EU GDPR). Developing a platform for regulatory learning, not only for the agenda-setting and lawmaking phases of the policy cycle, but also for the monitoring and enforcement phases, may lead governments to develop a much more effective approach to the post-deployment monitoring of AI systems. This may also extend to the issue of liability regimes for damage caused by AI systems, as well as its apportionment along the value chain—issues on which countries like Japan have provided important contributions in the form of guidance for drafting and implementing contracts related to data and AI.

3.1.4. A joint platform for regulatory sandboxes

The decision to prohibit a given AI application, classify it as risky, or otherwise regulate may occasion a need for experimental policymaking to foster innovation and agile regulation. Researchers and businesses interested in deploying such applications may face uncertainty about the risks and benefits or the applicability of particular regulation, or may disagree with its application and seek to demonstrate the possibility of using organizational and technical safeguards to establish the safety and trustworthiness of the AI system. Designing and implementing experimental schemes can be time consuming and require specific skills in design, execution, and outcome measurement.

To address such issues in the context of AI, a number of jurisdictions are adopting regulatory sandboxes to enable experimentation with AI applications in a controlled environment that can avoid certain legal risks. In 2019, the U.S. Consumer Financial Protection Bureau (CFPB) adopted a "Compliance Assistance Sandbox" for fintech that enables up to a two-year moratorium on certain regulatory requirements to enable testing where there is regulatory uncertainty.[189] Data protection authorities in the U.K., Norway, and France have adopted sandboxes to allow experimentation with AI that operates with personal information.[190] Korea and Colombia have done the same for AI experimentation in general.[191] The EU's proposed AI regulation encourages member states to adopt a form of sandbox that allows experimentation (with a priority for SMEs) under strict supervision, but only prior to any actual deployment.[192]

Given the complexity and resource-intensiveness of regulatory sandboxes, it would be extremely useful if FCAI governments could cooperate and even join forces, where needed, in testing the compliance of specific AI applications with rules or principles of responsible AI development. Progress on enhanced cooperation and possible convergence on risk management would open the possibility of launching international regulatory sandboxes to test AI systems with key requirements in a controlled environment. Besides facilitating a broadly converging approach to the policy and regulatory framework, the adoption of coordinated regulatory sandboxes for AI, as well as cooperation with sectoral regulators that have accumulated the most experience with other kinds of sandboxes and experimental policymaking (e.g., randomized controlled trials and adaptive regulation in health and pharmaceuticals, sandboxes in energy and finance, etc.), could become important points of reference for the community of AI developers and regulators.

Even without convergence on risk assessments or regulatory measures, an international platform for regulatory learning, involving all administrations that participate in FCAI and possibly others, appears to be a promising avenue for deepening international cooperation on AI. It offers potential cooperation opportunities independently of the approach adopted by individual countries (e.g., whether a more self-regulatory framework has been put in place, or regulatory requirements are aimed at specific AI applications considered risky). The platform could host an international repository of ongoing experiments on AI-enabled innovations, including regulatory sandboxes. As use of sandboxes becomes a more common way for governments to test the viability and

conformity of new AI solutions under legislative and regulatory requirements, updating information on ongoing government initiatives could save resources and inform AI developers and policymakers. Aligning the criteria and overall design of AI sandboxes among different governments would also increase the prospective benefits and impact of these processes, as developers willing to enter the global market might go through the sandbox process in a single participating country.

3.1.5. Cooperation on AI use in government: Procurement and accountability

A natural candidate for further exchange and cooperation in FCAI is the adoption of AI solutions in government. Such solutions include both "back office" systems designed to support internal administration as well as more public-facing applications for delivery of various government services and information. As major customers of such services, governments exercise significant influence over their deployment, and issues of ethical and trustworthy use of AI loom at least as large for the public sector as they do outside government. Countries like Canada and the U.K. have already adopted frameworks for the use of AI in government. In the U.S., the General Services Administration has established several "Centers of Excellence" to facilitate AI transformation by federal agencies.[193]

Exchanging good practices can also lead to a better understanding of the requirements for deployment of AI in government that makes the most of AI solutions and aligns with broader policy goals. Despite divergences in administrative law and in approaches to fundamental rights, enhanced cooperation on how public administrations can and should use AI would lead to a stronger dialogue and empowerment of civil society on issues related to the use of technology in support of public services. The sharing of good practices and overall lessons on what works when deploying AI in government would also be an important achievement. Important areas in this respect are procurement and effective oversight of accountability after deployment:

- **Procurement.** In many cases, governments will procure AI from third parties. As a significant portion of the economy in all FCAI governments, public procurement makes a powerful market-shaping instrument that can steer the entire AI market towards alignment with ethical and trustworthy AI development. Various recent initiatives have started to shed light on specific safeguards that governments should build into the public procurement requirements for AI systems. These include most notably the guidelines developed by the World Economic Forum Centre for the Fourth Industrial Revolution, in consultation with a multistakeholder community and in cooperation with the U.K. Government's Office for AI, Deloitte, and Salesforce;[194] and the "AI and procurement primer" developed by New York University.[195] Enhanced inter-governmental cooperation has the potential to shed more light on these processes and enhance the effectiveness and influence of public procurement.

- **Accountability.** The diffusion of AI systems into the work of government will likely put policymakers under pressure to monitor a constantly evolving operation of these systems. Like many AI best practice

The sharing of good practices and overall lessons on what works when deploying AI in government would also be an important achievement.

frameworks, both the U.S. GAO Accountability Framework and the EU AI Act include monitoring as a key requirement of any risk management plan for AI systems. Because of the importance to these governments and others of fairness, due process, nondiscrimination, and human-centered AI, they face a heightened need to practice what they preach by ensuring the AI that they deploy is ethical and trustworthy. Accordingly, public procurement requirements for AI—especially those in law enforcement or the delivery of services to citizens—should incorporate robust auditing and transparency requirements that apply continuously after deployment. This is complicated for many reasons. First, checking ongoing compliance with requirements requires access to the functioning of AI systems in addition to their output. Second, such continuous monitoring could be performed by the AI developers or deployers, but government purchasers would then need to establish checks on their diligence in order to monitor the evolution of the market—otherwise they will only be able to act post hoc, when damage materializes. Third, in a world with many interacting AI systems, determining the causal nexus between the operation of one or many AI systems and damage that has materialized might prove very difficult.

3.1.6. Sectoral cooperation on AI use cases

In the design of a policy framework for AI, countries can opt for horizontal, cross-cutting legislation or for a more sector-specific approach. This is not very different from what has already occurred in other cross-cutting domains of law, such as data protection. The European Union has largely adopted a similar approach with its proposed AI regulation—whereas the United States (and to some extent Canada and Singapore) appear to have taken a more sector-by-sector approach with some degree of central coordination.

There are pros and cons to both approaches. Adopting a sector-specific approach can ensure higher levels of regulatory certainty and adherence to existing business models, products, and services. Some examples are discussed below:[196]

- In sectors like **finance**, key criteria such as fairness, discrimination, and transparency have been subject to extensive regulatory intervention in the past, and sectoral regulation must ensure continuity while at the same time accounting for the increasing use of AI. In the United States, the five largest federal financial regulators released a "Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning" in March 2021.[197]

- In **health and pharmaceuticals**, the use of AI both as a stand-alone solution and as embedded in medical devices has prompted a very specific technical discussion regarding the risk-based approach to be adopted. This has already led to important sectoral initiatives such as the U.S. Food and Drug Administration's April 2019 discussion paper on a "Proposed Regulatory Framework for Modifications to Artificial Intelligence/Machine Learning-Based Software as a Medical Device," which prompted the adoption of an "Artificial Intelligence/Machine Learning (AI/ML)-Based Software as a Medical Device (SaMD) Action

Plan;" and the EU medical devices regulation, which entered into force on May 26, 2021.[198] In Japan, the risk classification system in this sector is slightly different from that of the U.S. and the EU, as shown in the figure below.

Figure 4. Medical Devices classification in the U.S., Japan, and the EU

Country [Regulator]	Medical devices classification				
United States [FDA]	Class I	Class II			Class III
Japan [Review: PMDA] [Approval: MHLW]	Class I	Class II	*	Class III	Class IV
European Union [Notification body]	Class I	Class IIa		Class IIb	Class III

Needs approval **Needs third-party certification** **Needs notification/self-certification**

* Medical devices for which certification standards do not exist (e.g., AI medical devices as of 2020)

Source: Aisu et al. (2021)[199]

On the other hand, there are also merits in a cross-cutting regulatory framework in rapidly-evolving fields. In particular, the blurring boundaries between sectors and the emergence of versatile, eclectic AI systems that can be applied to different use cases suggest a purely sectoral approach may not be sufficient to keep pace with market evolution. Also, the adoption of differing standards and criteria in the regulation of different sectors may increase regulatory costs for developers that serve more than one sector with their AI solutions. Moreover, in such a cross-cutting framework, examples from mature areas of regulation such as those illustrated above (finance and health) can also become a form of regulatory sandbox to model regulation for other sectors in the future.

Accordingly, the dichotomy between a sectoral and a cross-cutting approach to AI policy is not as significant as it may appear at first blush. Countries seem to be adopting a mix of both: for example, the EU AI regulation will now have to be adapted to sectoral regulation, an activity that is going to become more intense over the coming months; and the U.S. OMB guidance for federal agencies provides a degree of horizontal coordination and definitions, which reduce the possible divergence across sectoral regulators.

The dichotomy between a sectoral and a cross-cutting approach to AI policy is not as significant as it may appear at first blush. Countries seem to be adopting a mix of both.

3.2. Cooperation to enable sharing of data across borders

Data governance is a foundation for managing information. Privacy and data protection, cybersecurity, information systems, and digital strategies more broadly all require that an organization understand what data it has, where the data comes from, how that data is used and what happens to it, and who has access to the data. As many entities subject to the EU's GDPR discovered as they prepared for it to take effect, these questions require careful mapping of data flows inside and outside the organization throughout their lifecycles and consideration of the provenance, quality, uses, sharing, protection, and deletion of data.

This central role for data governance carries over to AI because data is its essential input and data governance can have broad impacts on how AI operates. The draft EU Data Strategy reflects a need to increase access to data;[200] and an MIT Technology Review survey of over 1,000 AI business leaders around the world found that 64 percent believe more regulatory clarity on data sharing is needed.[201]

Data governance is closely tied to regulatory policy, but warrants a separate discussion because of the importance of data to AI and because, unlike many of the policies discussed above, data governance is the subject of well-developed legislation and regulation and of discussions in several existing channels. Below, we focus on data sharing because it is where differences in data governance can impede effective development of AI. Effective international cooperation on AI needs a robust and coherent framework for data protection and data sharing. There are other significant data governance issues that may benefit from pooled efforts across borders that, by and large, are the subjects of existing international cooperation:

- Important data governance issues such as provenance, quality, and representativeness are under discussion by the GPAI working group on data governance.[202]

- Like data protection regimes, intellectual property laws can affect AI R&D, and the extent of alignment in such laws will affect AI collaboration and trade across borders. Since patent and copyright laws have a long history, it has been possible to achieve significant harmonization through treaties as well as regulatory cooperation. The rapid growth of AI patents may test these mechanisms, but, in light of the general alignment and existing channels, we do not see a role for FCAI in this field.[203]

- As technologies are shared across borders, global networks face rapidly evolving transnational threats to information security.[204] These call for deep cooperation among allies and trading partners. This subject by itself is broad enough to warrant its own set of dialogues outside the FCAI. We therefore leave this to another forum.

3.2.1. Privacy and data protection

Contrasting legal regimes on the use and protection of personal information have great potential to impede international cooperation on AI. This comes about for several reasons. First, unlike most other aspects of regulation affecting AI, privacy, and data protection, legal frameworks are well-developed in many countries. Second, these laws govern personal information in many spheres where AI can be valuable, such as health. Even in other contexts, such as transportation, where the identification of individuals is often unnecessary, the ability of advanced analytics to isolate unique patterns and thereby identify individuals even from "anonymous" datasets brings privacy and data protection to bear. And finally and most significantly from the standpoint of international AI collaboration, numerous such legal regimes limit flows of personal information beyond national borders. The impact of privacy on access to data and its use for AI highlights how different approaches may affect AI development and international cooperation.[205]

The EU's GDPR stands out as the most significant such regime because of its global ambition and reach, a product of the EU's gravitational force as a trading partner, which is reinforced by two aspects of the regulation: its extra-territorial reach, and the fact that it limits the transfer of personal data from within the EU to non-EU states ("third countries") unless the European Commission has reached an "adequacy" decision (i.e., a determination that the legal protections afforded to personal data are "essentially equivalent" to those under the GDPR).[206] Although the U.S. has numerous federal and state privacy laws governing use of personal information in various sectors or contexts, it has no comprehensive federal law covering nongovernmental sectors comparable to the GDPR. To put in place protections equivalent to those under EU law, the U.S. and EU arrived at the 2000 Safe Harbor and 2016 Privacy Shield frameworks.[207] These incorporated principles of EU data protection law, which allowed subscribing companies to transfer personal data from the EU to the U.S. if they incorporated the principles into their privacy policies, thereby making them legally enforceable by the U.S. Federal Trade Commission.

The EU's data transfer framework is not the only one. Numerous countries have adopted data protection laws with parallel limitations. The Asia Pacific Economic Cooperation group (APEC) has developed "Cross-Border Privacy Rules" (CBPR), a set of privacy principles and accountability practices enforced by an agency and an independent accountability agent designated by each participating government.[208] The principles are designed to ensure that data transfers meet a consistent level of protection even if national laws provide less protection. Nine APEC members—Australia, Canada, Japan, Mexico, South Korea, the Philippines, Chinese Taipei, and the U.S.—have taken the steps to join the CBPR system, and the U.S.-Mexico-Canada Agreement recognizes respective compliance mechanisms for transfers of personal data between those countries.[209] In addition to these mechanisms in place for transnational transfers of personal information, there are international frameworks developing along similar lines. During the Japanese presidency of the G-20 in 2019, Prime Minister Shinzo Abe made a broad call for "a new track for looking at data governance," which he labeled "data free flow with trust."[210] The G-20 leaders' "Osaka Declaration on the Digital Economy" recognized

The impact of privacy on access to data and its use for AI highlights how different approaches may affect AI development and international cooperation.

the importance of cross-border data flows as well as challenges to privacy and other values.[211] Work to advance data free with trust has continued through the World Economic Forum.[212]

The "Schrems II" judgment by the Court of Justice of the European Union (CJEU) in 2020, however, has been a seismic event for international transfers of personal information, the aftershocks of which are still reverberating and magnify the impact of the EU regime. The headline of the decision was its invalidation of the Privacy Shield framework for data transfers to the United States on the basis that U.S. intelligence agencies may have legal authority to access such data and EU data subjects are not guaranteed redress in U.S. courts. However, the court also addressed the model contract clauses that provide the main vehicle for companies of all kinds in the EU to transfer personal data outside the EU, including to Australia and Singapore among FCAI participants. Taken as a whole, the judgment could significantly curb flows of personal data beyond the boundaries of the EU.[213] The European Commission has adopted revised model clauses that include a menu of safeguards, and the European Data Protection Board, the collective body of EU data protection regulators, has issued its own parallel guidance.[214] These safeguards and the CJEU's standards set a high enough bar to curtail transfers, at least to the U.S. and to countries that engage actively in surveillance of online communications.[215] The effect is what Georgetown Law professor Anupam Chander terms "soft data localization."[216]

The U.S. is handicapped in advocating for free flow of data so long as it remains an outlier on privacy and data protection compared to its leading allies and trading partners. Conversely, the EU's GDPR inhibits data sharing and AI development in important respects.

The European Commission and U.S. government are in active discussions toward a new data transfer framework specific to the U.S. In addition to these discussions on commercial data sharing, the OECD has initiated a process to explore norms on the scope and safeguards for government access necessary in democratic states.[217] Signatories to the Budapest Convention on Cybercrime are working towards a "Second Additional Protocol to address access to legal evidence and cooperation.[218] The stakes for these discussions are magnified by developments in countries that are adapting GDPR-like legislation for data protection in ways that can enable authoritarian power. As noted, China's new data protection law will become effective on November 1, 2021 and India is also considering data protection legislation. Even as their draft legislation proposes strict protections for personal information for enterprises, they also incorporate explicit requirements for data localization.[219]

The United States is handicapped in advocating for free flow of data so long as it remains an outlier on privacy and data protection compared to its leading allies and trading partners. While many privacy concepts and practices originated in the U.S.,[220] growing gaps in existing sectoral laws allow U.S. companies wide room to set their own rules. Without a comprehensive privacy law filling these gaps in the commercial sector, the U.S. comes to the discussion table on international data transfers with diminished standing. With respect to government access, the safeguards and transparency circumscribing the U.S. intelligence community set a standard for the world,[221] but it may need to codify these safeguards into law to make them clear to the world. The U.S. may be able to reach an accommodation with the European Commission, through legally binding principles for companies and administrative measures for surveillance, that can serve as the basis for a new

adequacy decision. Such a decision inevitably will be subject to legal challenge. However, it could furnish a stopgap toward a broader and more stable framework for international data exchanges.

Conversely, the EU's GDPR inhibits data sharing and AI development in important respects. Data protection regulators have interpreted the grounds for processing data and the scope of permissible technical and administrative measures to de-identify personal information very narrowly. The effect has been to expand the circumstances in which consent from a data subject is necessary and contract the range of uses of data considered consistent with the original purpose of processing. These limit the ability to engage in data discovery that is vital to the data science that is a pillar of AI. The treatment of research uses under the GDPR may offer some mitigation for these restrictions in the context of AI research and development. The GDPR allows some latitude for organizations that conduct scientific, historical research to avoid consent for use of data in sensitive categories and certain other limits on use and retention of data.[222] Most significantly for purposes of international collaboration, Article 49(h) permits transfer to "third countries" in limited circumstances.

During the COVID-19 pandemic, the GDPR's treatment of research has provided a framework to address the exigencies of public responses.[223] Where there are less compelling exigencies for research, however, this latitude may not be available as readily in other fields. Despite this latitude, moreover, the European academy networks—ALLEA (the European Federation of Academies of Sciences and Humanities), EASAC (European Academies' Science Advisory Council), and FEAM (Federation of European Academies of Medicine)—jointly issued a consensus report in April 2021 concluding that "[i]t has become apparent that the implementation of the GDPR has introduced impediments to…international transfer of data outside the EU/EEA, creating problems for academic researchers, health care professionals, and others in the public health sector" with "no workable mechanism for sharing health data for public sector research."[224] This warning for an area of research privileged under the GDPR indicates greater impediments for other areas of research. As both the European academies and the International Science Council stress, research data constitutes a global public good.[225]

As a review of the GDPR has already started in the Commission in accordance with the provisions of Article 97, the time is ripe to consider how to reconcile the principles and objectives of the GDPR with the goal of facilitating research around the world. These issues also extend to the revision of standard contract clauses for transfers of data outside the EU and to , as well as the measures that EU authorities consider as "additional safeguards" for protection of personal data while enabling cross-border data sharing for research purposes.

3.2.2. Opening government data

As governments develop the national artificial intelligence strategies described in Section 2 (page 26), an important facet is the expansion of access to large datasets. Governments have long been in the business of collecting and reporting data from both subgroups and the overall population, including data related to demographics, public health, finance, climate, law

enforcement, transportation, education, and housing. Government data has proved to be a significant resource for academics or industry researchers when accessible for digital re-use.

The value of data for AI and other digital development has increased the focus of FCAI governments in opening use of government datasets to the general public:

- Australia's 2015 "Public Data Policy Statement" pledged to make non-sensitive, anonymized data open by default, and the government currently maintains approximately 100,000 research datasets on data.gov.au. A Data Availability and Transparency Bill seeks to expand access to public sector data for accredited researchers.

- Canada convened a Multi-Stakeholder Forum on Open Government[226] in 2017 to advise open government activities, and it laid out goals in its 2018–2020 National Action Plan on Open Government to improve open.canada.gov and expand the "Open By Default" pilot project.[227]

- The EU established the "Open Data Portal"[228] in 2012 to expand access to public datasets and released the European Strategy for Data in 2020 that aims to "invest in a High Impact Project on European data spaces and federated cloud infrastructures" to facilitate data sharing between EU member states.[229] In November 2020, the European Commission proposed a Data Governance Act to establish rules for the sharing of data in private hands as well as the reuse of government data, and establishing a European Data Innovation Board.[230]

- Since Japan's release of its Open Government Data Strategy[231] in 2012, the government has maintained public, machine-readable datasets and statistics from the central government on data.go.jp and e-stat.go.jp/en, respectively.

- Singapore's Government Technology Agency has maintained data.gov.sg since 2011, which currently holds over 30,000 open datasets from 70 public agencies and launched a resource page in 2016 with 16 different APIs.[232]

- The U.K.'s open data efforts date back at least a decade, when the government launched data.gov.uk in 2010 and published a 2012 white paper on the benefits of data sharing.[233] The U.K. also set goals in the 2017 Government Transformation Strategy[234] to develop an open data agenda to focus on high-priority efforts; in the 2019 AI Sector Deal[235] to create interoperable, open data standards; and in the 2020 National Data Strategy[236] to "ensure that public sector data is the backbone of innovation, efficiency, and growth."

- Supported by the 2018 OPEN Government DATA Act, which requires federal agencies to publicly release government datasets in standardized formats, GSA currently manages the data.gov website which contains approximately 300,000 government datasets and open-source code from across the U.S. federal government.[237]

These initiatives provide a valuable foundation for AI data needs. Building on this foundation will require attention to the international dimensions of data sharing, which present technical as well as political challenges.

3.2.3. International data sharing

As governments expand the availability of data, they should also consider how to multiply the impact of public sector datasets by sharing them beyond borders. International data sharing is beneficial in the current global efforts to fight public health and climate change crises; for example, the U.S. government has collaborated with Singapore and Germany to launch the Global Initiative On Sharing Avian Influenza Data, and similarly with the DNA DataBank of Japan and European Nucleotide Archive to launch GenBank, in order to improve global access to COVID-19 data.[238] The 2015 Paris Agreement urges signatories to improve information sharing, among other practices, in order to fight global warming and reduce greenhouse gas emissions.

The EU's proposed Data Governance Act contains significant proposals to expand the availability of public sector data as well as data in the hands of the private sector; however, proposed limits on transfers outside the EU may restrict international sharing of data, including for purposes such as health research.[239] Just as the time is ripe to consider the impact of data transfer rules in the GDPR on global research, debate on the DGA should weigh the objectives of similar rules against the benefits to research and development of AI.

3.2.4. Improving data interoperability

Despite its benefits, the value of international data sharing is complicated by issues of data formatting and harmonization, in addition to the need to protect data security and privacy. Opening government data to the public is insufficient by itself to make it interoperable, especially in international contexts. There are additional requirements to enhance international data sharing in meaningful ways. Government data must first be interoperable in its format. Creating wide consensus around specific data formats is challenging, but some shared data formats can become prevalent enough to enable international interoperability. A notable example is the General Transit Feed Specification (GTFS),[240] which has become a de facto world standard for sharing local government transit data. Originally started by a collaboration between the city of Portland, Oregon and Google,[241] GTFS sought to enable easier trip planning on public transit systems. Now the format is used by hundreds of local governments in over 50 countries, and its use is encouraged by institutions such as the World Bank.[242] The consistency of this data is what enables trip planning on public transportation systems using popular mapping and navigation apps.

While data formatting can be a complex barrier to interoperability, creating consistency in the actual meaning of the data is frequently a far greater challenge. Data is defined by the minutiae of how it is collected—the criteria that lead to a data entry, the mechanics and environment of sensors or other collection devices, the units of measurement, the languages, and the relevant human processes. Data harmonization, through which different

data sources are combined in a way that their contents are meaningfully comparable, is not a purely technical challenge, as the choices on how to collect, store, and exchange data frequently reflect policy priorities of local governments. These choices are often tied to legacy digital infrastructure, pre-existing paper forms, manual data entry processes, software procurement, languages, parochial needs, and other factors that are not easily changed. Data harmonization is therefore especially challenging when data is collected by sub-national governments, which multiplies the challenges of these factors for consistency in policy choices.

The case of low-cost air quality sensors, which have recently emerged as a dramatically cheaper alternative for measuring air pollution, is an example of the challenges of data harmonization. The hardware used by low-cost air quality sensors varies substantially, which affects the manner of pollutant detection, the units and rates of measurement, and other important details.[243] The various sensors' measurements are also affected by factors like the environmental temperature and humidity,[244] which are in turn affected by human choices such as the sensor's proximity to roads and the height at which it is placed.[245]

Often, extensive efforts are necessary to enable comparisons, as is the case with global air quality measures. Since low-cost sensors are also less accurate than the traditional reference-grade air quality sensors, the low-cost versions must be calibrated, often using machine learning,[246] through a process that varies based on locality.[247] This type of data harmonization challenge is the norm, not the exception, and open data should never be assumed to be automatically comparable across different governments and data collection processes. Governments—especially smaller ones—can enable better data sharing by documenting open data in data dictionaries that thoroughly describe the meaning of data values and the data collection processes. Still, considerable technical effort is necessary to foster international sharing of government data. Thus, data sharing projects should be carefully prioritized and sufficiently supported.

3.2.5. Improving technologies for trustworthy data sharing

It is important for governments to address ways to maintain the privacy and security of personal information while simultaneously encouraging data sharing. As noted in Section 3.2.1 (page 61), increases in the availability of data and computing power have made data more vulnerable to the identification of unique records that can link back to individuals even when identifiers have been removed. In addition, government computer systems have been prime targets of cyberattacks that can threaten the availability or integrity of public data. The Center for Strategic & International Studies estimates that over 80 "significant" data breaches have occurred worldwide from January to July 2021 alone—many of them targeting government agencies—which have cost victims over $1 million each.[248] The high potential financial, reputational, or other costs of privacy and security breaches, coupled with the increasing frequency and complexity of cyberattacks, call for better methods to protect against these risks.

To protect the confidentiality of personal information, governments can use technical methods—known as privacy preserving computation (PPC) techniques—to enable third-party researchers to grant access to data analysis with third-parties without actually transferring the underlying data.[249] Some major PPC techniques include (a) differential privacy, which adds filler information to datasets to conceal any personal information related to individuals while still allowing researchers to analyze overall patterns; (b) homomorphic encryption, which allows researchers to analyze encrypted data without ever decrypting it throughout the process,[250] (c) multi-party computation, which allows multiple researchers to analyze their combined encrypted data without revealing the input data that each holds; (d) blockchain, which decentralizes data transfer and storage and thus distributes any security risks over multiple points of failure;[251] and (e) federated databases, which connect multiple databases that are physically located in different places, enabling researchers to analyze the overall data without either transferring or duplicating it across databases.[252] However, many of these PPC techniques are complex, cumbersome, and computing-intensive, resulting in slow development and uptake among the public and private sectors.

Yet there are examples of FCAI governments, including Australia, the EU, Singapore, the U.K., and the U.S., incorporating PPC techniques into their operations:

- In 2016, the Australian government established Data61, a data science branch of the Commonwealth Scientific and Industrial Research Organization (CSIRO), which is developing PPC technologies like federated systems.[253] Data61 is collaborating with the Australian Federal Police and Monash University to develop "Data Airlock," a "Model-to-Data" algorithm that protects privacy while scanning photos during police investigations,[254] and the Australian Transaction Reports and Analysis Centre (AUSTRAC) is exploring the use of homomorphic encryption to work with third-parties to monitor patterns in financial transactions.[255]

- In addition to the European Strategy for Data, the EU has funded organizations or projects like ELIXIR, which is developing a federated database to share COVID-19 health data among EU member states; GAIA-X, which aims to create standards for a "federated open data infrastructure based on European values" to enable secure data sharing within the EU; and MyHealthMyData, which explores health data anonymization through blockchain, homomorphic encryption, and multi-party computation.

- AI Singapore (AISG) established both the "Federated Learning Lab" and a federated learning system called Synergos;[256] the Singaporean government has also announced the launch of two new research centers that will work on privacy-preserving technologies, as well as a S$50 million investment from 2021-2026 to improve public trust in technology, including developing privacy-preserving technologies.[257]

- The U.K.'s gov.uk "Verify" feature utilizes a federated learning system to allow third-parties to confirm identities of people who wish to file taxes or access other online government services,[258] and the Cyber Defence Alliance is reportedly either testing or using homomorphic encryption to collaborate with third-parties on fraud and cyber investigations.[259]

- The 2020 U.S. Census used differential privacy and encryption to protect collected personal information, which it has described as the "world's first large-scale application" of such a differential privacy system.[260] Meanwhile, the U.S. National Security Commission on Artificial Intelligence (NSCAI) released a report in March 2021 that called for default incorporation of federated learning and data minimization into government databases.[261]

Others, such as Canada and Japan, are exploring the use of these technologies. The Office of the Privacy Commissioner of Canada released a report on privacy-enhancing technologies in November 2017, stating that "additional research is needed to assess [their] relative strengths and weaknesses,"[262] and wrote in an April 2021 blog post that federated learning, differential privacy, homomorphic encryption, and secure multiparty computation are still under development and not yet widely-deployed.[263] Meanwhile, the CIFAR Pan-Canadian AI Strategy recommends increasing "access to high-quality and fully traceable federal data, models, and computing resources while maintaining safety, security, privacy, and confidentiality protections," and conducting "research into new ways of protecting privacy."

Japan's Committee on Personal Data Technical Working Group is exploring privacy-preserving technologies such as de-identification and encryption,[264] and the "Data Free Flow with Trust" framework published through Japan's 2019 G-20 leadership states that "governments should also ensure the availability of multiple [privacy and security] mechanisms and derogations for the cross-border transfer of personal data"; and "technical solutions can help deliver these guarantees—through solutions like federated data systems and homomorphic encryption—especially for cross-border purposes."[265]

In addition to public sector investment of PPC or privacy legal frameworks, governments also can encourage voluntary sharing of data held by the private sector. While it is not uncommon for companies to share advancements in AI through open-source software and publications, it is far less frequent to share data. Some large datasets, largely from academic origins, have been made publicly available, including datasets of 35 million Amazon product reviews[266] or the 14 million labeled images of the famous ImageNet dataset.[267]

However, companies normally see proprietary data as a competitive asset and rarely choose to give it away. Even so, it is possible for companies to use federated machine learning and other PPC techniques to learn from one another's data without allowing their competitors direct access. For example, in 2019, 10 pharmaceutical companies including AstraZeneca and Johnson & Johnson agreed to pool data from clinical drug trials while using federated machine learning to protect privacy and security—which could ultimately reduce the costs and speed of new drug development through AI.[268] In addition, private U.S. corporations like IBM, the caregiving platform Aviva,

the data sharing platform Ocean Protocol, and the health care platform Roche Diagnostics are each reportedly developing PPC technologies that incorporate federated learning and blockchain.[269] Governments should encourage these developments and types of partnerships when possible, and even consider actively engaging to help ensure their success, especially in areas imbued with the public interest like health, transportation, robotics, and energy systems, where data pooling could lead to enormous benefits for societies. The EU has taken a step in this direction in its Data Governance Act by proposing a category of "data altruism organizations" that would enable individuals or organizations to pool data for reuse in research or for other public purposes.[270]

3.3. Cooperation on international standards for AI

As countries move from AI ethical principles and policies to more concrete efforts to regulate AI, the demand for AI standards will grow. For example, the proposed EU AI Act is likely to drive demand for AI standards, including standards for risk management, data governance, and standards on the technical documentation that can establish compliance of high-risk AI systems with the Act.[271] Moreover, under the EU AI regulation, using AI standards creates a presumption of conformity, further incentivizing AI standards development and use.[272] International AI standards will also be needed to develop commonly accepted labeling practices that can facilitate business-to-business (B2B) contracting and to demonstrate conformity with AI regulations; to address the ethics of AI systems (transparency, neutrality/lack of bias, etc.); and to maximize the economic opportunities for AI globally. Developing international AI standards in standards development organizations, such as the ISO/IEC and IEEE, provides an opportunity to ensure that global AI systems are responsible and that the opportunities from AI are widely distributed.

Developing technically robust AI standards requires scaled efforts to gather data and undertake the research that can translate principles and emerging industry practices into AI standards that can be measured and assessed. This role is especially apt for AI because of its technical complexity and rapid evolution. The work needed includes research on common terminologies, definitions, and taxonomies of concepts applicable to AI systems—for example, the features that make up trustworthy AI and how these can be measured. As noted, ISO/IEC SC 42 is developing AI terminology and definitions. NIST is undertaking such work as part of AI Measures and Evaluation (AIME) work.[273] CEN-CENELEC has also commenced work on AI standards.

Developing technically robust AI standards requires scaled efforts to gather data and undertake the research that can translate principles and emerging industry practices into AI standards that can be measured and assessed. This role is especially apt for AI because of its technical complexity and rapid evolution.

This initial focus on terminologies, definitions, and taxonomies underscores the importance of a stepwise approach to AI standards development that is consistent with and supportive of stages of AI development. SDOs are also working on broader standards that are translating AI ethical principles into processes that industry can implement, working through the trade-offs and context specific issues that arise as AI systems are broadly deployed. For

instance, ISO/IEC AI standards on bias in AI systems and trustworthy AI as well as IEEE work on Model Process for Addressing Ethical Concerns During System Design all address the need for standards on trustworthy and responsible AI.

There will also be some need for sector-specific AI standards. Such standards can provide a common approach to measure the performance of an AI system and for developing protocols that build interoperability among disparate AI systems. The emergence of standards for autonomous vehicles (AV) provides a well-advanced example. Technical AI standards will be needed to ensure that AV run safely by describing requirements for test methods, that AV decisions in road traffic achieve consistent explainability and validation, and that AI systems in AV are interoperable with each other. Work is under way in ISO/IETC JTC1 on data management and interchange to address such issues.

International AI standards can also help minimize the trade costs associated with localized approaches to AI regulation discussed in Section 1 (page 16). International AI standards can enable global interoperability, both in terms of the technology, and the business management practices that will be needed to ensure its development and use is consistent with AI that is trustworthy and reliable.[274] This is particularly important as countries may otherwise develop their own AI systems in ways that are at odds with international AI principles of responsible AI development. Engaging with countries like China and Russia through the standardization process can be a useful way to nurture a truly global technical community working on AI development, thus attaining economies of scale and preserving the trade-enabling and competition-enhancing goals of international AI standards. Failure to agree on truly global AI standards could lead to the bifurcation of the technology stack at the technical or at the policy level.

Experience developing and using AI systems is also needed to establish the data and knowledge base that can lead to a standardized approach to AI systems. Data and experience with AI will need to be provided by academia, civil society, and government, as well as industry. This is particularly true for foundational AI standards that are cross-cutting and include terminology and definitions.

3.3.1. De facto industry standards

The central role of the private sector in developing and implementing technology has historically made industry a key driver of international standards in SDOs such as the ISO, IEC, and IEEE.[275] This will also be true for AI standards, where industry is leading in AI R&D and commercialization, including the business practices and management systems that can ensure safe and trustworthy AI. The different approaches among FCAI participants in these SDOs will often reflect progress among industry on developing their own AI technologies, which can drive the need for standards. Where industry-developed AI systems gain sufficient market share and user installed base, a "tipping" effect can lead them to become the de facto industry standard for a given system or market.[276]

For example, Microsoft showcases its use of AI across three categories: augmenting a company's human expertise (such as packaging buyer insights and recommendations for internal sales executives[277]), optimizing financial operations,[278] and utilizing bots to support a variety of tools and services supporting both customers and Microsoft employees.[279] Last year, IBM launched two information technology (IT) tools powered by AI. IBM Watson AIOps automates "the detection, diagnosis, and response to IT anomalies in real time," and its Accelerator for Application Modernization with AI supports clients seeking to elevate on-premises applications to function in a cloud-based workplace.[280] Google offers a substantial list of products powered by AI, including its dominant search engine, which has evolved to incorporate deep learning into its search algorithm, Google Ads, and Google Translate.[281]

Industry-led AI standards are also evolving using open-source software such as Google's TensorFlow and Facebook's PyTorch, which enable outside developers to use this software for their own AI challenges.[282] IBM has established high-level Principles for Trust and Transparency and deploys a comprehensive open-source toolkit for detecting bias in machine learning (ML) models and for explaining ML models and data.[283] Where these open standards are widely adopted, their network effects can also lead them to becoming de facto AI standards. Over time, these open-source standards may also come to be reflected in international standards developed in international SDOs such as ISO/IEC. This highlights the close link between industry AI development and international AI standards developed in SDOs. It also underscores the broader point that industry success with developing AI is key to leadership on AI standards.

3.3.2. AI in Standards Development Organizations: comparing national approaches

The seven governments participating in the FCAI recognize and support industry-led standards setting. While there are differences in how the FCAI participants engage with industry-led standards bodies, a common element is support for the central role of the private sector in driving standards, which marks a difference with the overall approach of other countries, such as China, where the state is at the center of standards making activities.[284] China's engagement on AI standards has potential implications for developing globally consistent approaches to ethical AI.[285] Therefore, in this section we compare emerging approaches in FCAI governments with the Chinese one.

When it comes to the ISO, IEC, and IEEE, representation and engagement is determined by each of their internal governance rules. IEEE membership is based on individuals, whereas ISO and IEC members are national standards bodies from 165 countries. For example, ANSI represents the U.S. standards body in ISO and IEC. EU industry is represented by national standards bodies and includes participation by CEN-CENELEC in ISO and IEC and ETSI in the 3rd Generation Partnership Project (3GPP). These EU standards bodies have codified cooperation with their international counterparts and represent EU interests in international standards bodies.[286] Australia, Canada, and the U.K. follow a similar approach, where Standards Australia (SA), the British Standards Institution (BSI), and the Standards Council of Canada (SCC) represent and promote national interests in ISO and IEC.

China is represented in ISO/IEC JTC1 by the Standards Administration of China (SAC) and by the China Communications Standards Association, which remains under the control of the Ministry of Industry and Information Technology.[287] The importance of international AI standards for China's successful globalization of AI will likely reinforce these private industry-state linkages and the development of a state-led strategic approach to the development of AI standards domestically and in international standards bodies.

Anecdotal evidence suggests that China's state-led approach in otherwise industry-driven SDOs such as ISO, IEC, and IEEE has not yet led to the developments in these SDOs of China-centric AI standards. This appears due to ISO/IEC rules of "one country, one vote," which so far has prevented China from dominating proceedings. Moreover, the emphasis in these standards bodies on expert driven, rules-based processes has also limited the scope for China to dominate, particularly where proposals are driven by a government agenda and are not technology-driven. In the IEEE, which is open to participation by individual experts, increased participation by representatives from China has increased scope for input. However, even here it seems that internal IEEE norms that emphasize expertise have managed, so far, to circumscribe China's or indeed any other single nation's influence.

This underscores the broader point as to the importance of SDOs' internal governance practices, including requirements for transparency and due process in the standards development process, as guardrails against Chinese government pressures to bend these organizations to meet geopolitical goals.

3.3.3. Implications for developing AI standards in international standards bodies

As industry develops AI systems, cooperation on international AI standards can provide the technical robustness to ground trustworthy and reliable AI. International AI standards also are needed so that businesses and consumers can understand and evaluate the trustworthiness and reliability of the AI systems they use.

As outlined, AI standards can play a range of roles when it comes to AI.

- At one end are the **foundational AI standards around terminology and definitions**: These AI standards will be needed before getting at the more complex issues. Progress on foundational AI standards will require further data gathering and research and requires a cooperative exercise by all FCAI participants. In this respect, the AI standards and processes for cooperation in international SDOs provide an important normative baseline and well understood and proven processes for reaching consensus on a range of AI issues.

- **AI standards that describe how AI systems work and the governance required to produce trustworthy and reliable AI** will require additional data and research as well as AI systems being sufficiently mature that there are use cases and some experience with the AI systems to understand what works and what is needed.

A key starting point for building international cooperation on AI standards is to strengthen the pace and capacity for AI innovation among FCAI participants. The ability to lead in the development of AI standards will indeed depend on the availability of domestic capacity for AI R&D and commercialization.

3.3.4. AI standards, international trade and geopolitical competition

The development of AI standards can support international trade and investment in AI, expanding AI opportunity globally and increasing returns to investment in AI R&D. The WTO TBT Agreement provides that members should use relevant international standards as a basis for their technical regulations, unless it can be shown the standards are ineffective or inappropriate.[288] AI standards developed in SDOs whose standards development processes meet WTO principles for international standards are directly relevant here.[289] However, the capacity of the WTO to support diffusion of international AI standards is limited by its application only to goods, whereas many AI standards will apply to services.

The ability for international standards to support international trade has also been premised on compliance with the broader set of WTO rules, including a commitment to reducing barriers to trade. Yet, China's approach to AI risks turning this link between standards and trade on its head. Specifically, China's aim to increase self-sufficiency along the AI value chain could undermine the capacity of AI standards to open markets and increase opportunities for international trade.[290] This mix between China's push for technology independence including with respect to AI, alongside its development of China-specific AI standards deserves scrutiny. On the one hand, where engagement in ISO/IEC helps integrate Chinese AI globally, it should be encouraged. On the other hand, there is risk that Chinese-specific AI standards could be used to support globalization of its own AI industry champions, while keeping its domestic market closed to foreign participation.

This underscores a broader point: that use by the Chinese governments of AI standards for broader strategic ends risks turning the industry-led, technology-driven approach to AI standards into a forum for geopolitical competition. The standards making process has never been entirely technical, with scope for politics and power to determine outcomes.[291] However, the industry-led nature and limits on state participation have kept the focus on technical expertise.[292] State rivalry in standards bodies could reduce the ability of these bodies to generate technically sound and research-driven results.

The industry-led nature and limits on state participation have kept the focus on technical expertise. State rivalry in standards bodies could reduce the ability of these bodies to generate technically sound and research-driven results.

The more direct engagement by the Chinese government in setting standards, driving the agenda, and aligning these with broader Chinese government priorities requires attention given the increasing control within private industry by both the Chinese Communist Party and the central government. As a result, technology-focused strategic competition with China risks spilling over into the work of international standards bodies on technology such as AI.[293] FCAI governments in their responses to Chinese government engagement in SDOs should not exacerbate the problem by ratcheting up government geopolitical competition within SDOs or slowing the international standards making process enough that AI standards are developed de facto

by industry players rather than through broad-based SDOs. Instead, FCAI governments should cooperate to support SDOs in adhering to industry-led, technically-oriented processes.

The absence of an effective international standards development process would likely accelerate adoption of AI standards developed by Chinese companies or the government, particularly by countries participating in the "Digital Silk Road," by which China aims to export internet infrastructure, promote e-commerce, and propagate its internet technology standards.[294] At this point, either outcome is possible—globalized AI standards or bifurcated AI standards centered around China on the one hand and the West on the other. Which outcome prevails will to some extent at least depends on progress setting international AI standards.

Developing international cooperation on AI would benefit from putting cooperation into operation with specific use cases.

3.4. R&D cooperation: Selecting international AI projects

The foregoing discussion demonstrates considerable high-level agreement among leading countries that international cooperation is desirable on AI in general and on values and policy principles for trustworthy AI. It also shows that differences in national interests and approaches to law and regulation—as well as perceptions of these differences—present obstacles to international cooperation. Even as we make recommendations for ways to bridge or minimize these differences, we acknowledge that differences in political interests, thinking about law and government, and fundamental beliefs may slow progress toward this goal.

We also perceive that progress may be slowed by the challenges of resolving differences only in the abstract, with no focus on concrete use cases. Productive discussion of AI ethics, regulation, risks, and benefits requires use cases because the issues are highly contextual. As a result, AI policy development has tended to move from broad principles to specific sectors or use cases. This trajectory is evident in the EU's progression from a goal of broad legislation on "the human and ethical implications of [AI]" in 2019 to a white paper in 2020 and proposed legislation in 2021 focused more narrowly on identifying sectors and applications that present high risks to safety or fundamental rights.[295] Similarly, the White House went from a broad survey of issues in 2016 to regulatory guidelines in 2020 aimed at risk-based application by regulatory agencies within their sectors.[296] A major element of Singapore's artificial intelligence strategy is to develop AI through sectoral projects: freight planning, municipal services, personalized medicine, border security, and disease prevention.[297] GPAI priorities have evolved from initial projects mainly about AI toward emphasis on "very concrete and unique use cases" in 2022, with "moonshots welcome."[298]

Considering this need for concrete context, we suggest that developing international cooperation on AI would benefit from putting cooperation into operation with specific use cases. To this end, we propose that FCAI participants expand efforts to deploy AI on important global problems

collectively by working toward agreement on joint research aimed at a specific development project (or projects). To paraphrase one participant in our dialogues, international discussions talk a lot about cooperation, but need to show actual cooperation. The parameters for such a project will be a subject of further dialogues among officials and experts, and will need to take into account important proposals for international collaborative R&D among several governments and multilateral bodies, including GPAI. In this report, we outline some of the considerations and issues for future discussion.

First, we articulate criteria for the kinds of goals or projects to consider, which align with those articulated in the GPAI 2022 priorities. Additional discussion and research will be needed to explore what areas of R&D fit these criteria and can attract support from governments and stakeholders. In addition discussions should explore how to build on and complement ongoing initiatives in GPAI and other international bodies to harness AI toward the SDGs and problems like climate change and global health.

Global significance. Such a project should be aimed at important global issues that demand transnational solutions. The shared importance of the issues should give all participants a common stake and, if successful, could contribute toward global welfare. Potential areas of focus could be climate change, public health, or improved modeling of economic growth and development.

Global scale. The problem and the scope of the project should require resources—funding, access to data, computing power, knowledge, and talent—on a large enough scale that the pooled support of leading governments and institutions adds significant value.

A public good. Given its significance and scale, the project would amount to a public good for which private sector players have neither the resources nor the financial incentives to pursue on their own. In turn, the output of the project should also be a public good and both the project and the output should be available to all participants as well as used to improve access to data, talent, and computing capacity in less developed countries.

A collaborative test bed. Governance of the project is likely to necessitate addressing regulatory, ethical, and risk questions in a context that is concrete and in which the participants have incentives to achieve results. It would amount to a very large and shared regulatory sandbox. Ambitious collaborative projects like CERN and the U.S. space program also have demonstrated the ability to spin off side benefits as they solve identified problems through advances in science and technology.

Assessable impact. The project will need to be monitored commensurately with its scale, public visibility, and experimental nature. Participants will need to assess progress toward both defined project goals and broader impact in addressing ethics, risk, regulatory issues, and other collateral goals. Lessons from the projects should be shared widely.

A multistakeholder effort. In light of its public importance and the resources it should marshal, the project will need to be government-initiated. But the architecture and governance should be open to nongovernmental participation on a shared basis, and government engagement should act as a force multiplier for ongoing efforts. Input of the global AI research community will be vital to collaboration and results.

This proposal could be modeled on several large-scale international scientific collaborations: CERN, the Human Genome Project, or the International Space Station. It would also build on numerous initiatives toward collaborative research and development on AI. A notable one was launched by the International Telecommunications Union and other U.N. agencies in partnership with the XPRIZE Foundation: As a result, the United Nations hosted an AI for Good Global Summit aimed at harnessing data in support of the SDGs.[299] This has ongoing focus groups on health, 5G and other communications networks, autonomous and assisted driving, environmental efficiency for technology, disaster management, and open data. France has launched an AI for Good initiative also focused on the SDGs, seeking to steer French and other European AI developers into projects with impacts on health, education, and the environment. In addition, some private companies—including Google, IBM, Huawei, and Microsoft—have AI for good programs that apply AI resources to toward societal problems and partner with academia and civil society.

Much along the lines of this proposal, the Confederation of Laboratories for Artificial Intelligence in Europe (CLAIRE), an organization of research groups and individual researchers, has proposed a pan-European network and research center along the lines of CERN to focus on AI in earth observation for climate change, which has received €50 million from the European Commission.[300] While this idea is conceived as a means of strengthening Europe's AI development, it could be adapted to global scale. In a similar vein, one of the work streams of the GPAI Working Group on Responsible AI is an "action-oriented" project aimed at AI development for climate action and preservation of biodiversity. In addition, the U.S. NSCAI final report included significant recommendations for R&D collaboration, establishment of a multilateral research institute within the U.S. to collaborate with other international partners, and to support of the work of GPAI and the OECD through formal relationships with the U.S. National Research Institutes under the U.S. National Science Foundation. These initiatives lay groundwork for the sort of multilateral and multistakeholder collaboration we envision.

We note that each of the international scientific projects mentioned above flourished in the 1990s, in a unipolar world ordered by what was perceived to be a global consensus with expanding multinational bodies (although CERN was founded several decades earlier). In that new and optimistic era, U.S.-Russia cooperation in space programs was a powerful symbol in contrast to the "space race" during the Cold War. This year, Russia announced it will withdraw from the International Space Station by 2025.

Global collaboration on similar projects will be more difficult in a world of increased geopolitical and economic competition, nationalism, nativism, and protectionism among governments that have been key players in these

Global collaboration on similar projects will be more difficult in a world of increased geopolitical and economic competition, nationalism, nativism, and protectionism.

efforts. As the editors of Nature recently commented, "there are signs that mounting geopolitical tensions—particularly between the United States and China—might be diminishing the exchange of people and knowledge between nations." They went on to add, "effort is needed on all sides to strike an appropriate balance that safeguards the great rewards that flow from mutually beneficial cooperation between researchers." Even so, the kinds of problems that should be the focus of potential projects are ones where China could make a valuable contribution.

Here, President Kennedy's famous words about the U.S. space program are apposite: "We choose to go to the moon in this decade and do the other things, not because they are easy, but because they are hard, because that goal will serve to organize and measure the best of our energies and skills."[301] The same can be said of a project to harness the power of AI toward solving global challenges. Not only would it test the possibilities of AI, but it also would test governments' commitment to solving these challenges, and doing so cooperatively, and demand additional commitment to solving operational issues along the way.

4.

RECOMMENDATIONS

By default, AI's advancement and development, its scientific and beneficial use, and its risks and challenges have few natural borders in either the digital or physical global markets for AI systems. Yet today, over 60 countries have adopted a national AI policy, advancing their own funding, development, standards, and direction around the use of AI. This explosion of AI policy may result in divergence and complexity that, without international cooperation, can lead to conflicting and counter-productive national policies.

Cooperation can bring the benefits of scale to AI research, advance ethical AI through shared principles and mutually reinforcing rules, ease trade for AI-driven products and services, untap the potential of AI for global challenges, and ensure AI does not undermine democratic regimes and values. Conversely, the lack of collaboration can bring about the opposite—inconsistent and less effective administration of responsible AI practices, unnecessary barriers and costs for trade and innovation, a more fractured internet, and an incoherent alternative to digital authoritarianism. By prioritizing regulatory alignment, shared standards, and AI projects for global good, the governments of FCAI can collectively mitigate the harms while reaping the benefits of AI.

FCAI governments are exploring many policies for AI, including U.S. agencies developing sectoral guidance, the EU's proposed requirements on high-risk AI, and Singapore's self-regulatory approach. At the same time, there is growing recognition across FCAI governments, as well as other participants, of the need for collaboration on regulatory policies, on AI standards, and in validating AI for good through practical and scalable projects.

When it comes to cooperation on AI policies and regulation, complete regulatory alignment is unlikely, though governments can agree on many fundamental components, including AI definitions and principles, a consistent framework for assessing AI risk, common approaches to testing and auditing AI, sharing AI successes and failures, and building channels for collaboration by sectoral regulators. Collectively, these steps forward can meaningfully unify these countries in a cohesive approach to AI governance, without unnecessarily restraining unique national regulatory developments.

As AI is incorporated into more products and services, demand for AI standards is expected to rise, resulting from both the private sector's interest in interoperability and the public sector's need for AI standards to underpin regulatory requirements. Industry-led AI use is quickly evolving into de facto global standards, through market dominance, prevalent use of open-source software, and adoption by competitors. A range of international standards bodies are also actively working to shape the emerging field with general support by FCAI governments, which may assist transnational alignment of AI use within industries.

To enhance the development of international AI standards, FCAI governments can fund national standards bodies to work on AI definitions and evaluation metrics, identify new priorities for AI standards, share data and progress with other governments, support academic and industry participation in SDOs, and include AI services in trade agreements such as occurs for goods in the WTO TBT Committee. China has attempted to influence international SDOs in a self-serving way that has raised alarm among trade competitors; FCAI governments should cooperate in

supporting SDOs that are industry-led and technically-oriented organizations while encouraging Chinese participation consistent with an industry-led approach to setting international AI standards.

Moving past discussions of AI standards, policies, and regulations toward collaborative projects would further AI's global benefits and enable tighter international alignment. There are many examples of global challenges that would benefit from the combined efforts of FCAI and other nations—especially those where shared data provides a significant advantage. In addition to advancing AI in combating mutual challenges, these projects could also help overcome political obstacles to international cooperation on AI. Multistakeholder projects of global scale and significance, aimed at a broad public good could help unify the world's approach to AI. The selection of these projects should be led by scientists, but policymakers should look to fund worthy candidates, such as using AI in earth observation and climate change studies—a current focus of both international scientific and policy collaborations.

The dialogues and associated research work of the Brookings-CEPS FCAI have deepened our conviction that global AI governance will benefit tremendously from additional discussion, collaboration, and alignment.

The dialogues and associated research work of the Brookings-CEPS Forum for Cooperation on AI have deepened our conviction that global AI governance will benefit tremendously from additional discussion, collaboration, and alignment. Many policymakers and experts have expressed uncertainty about the perspectives, approaches, and goals of other nations on a range of AI topics—uncertainty that this forum seeks to mitigate. Despite broad endorsements from FCAI participants of international collaboration, specific and appropriate steps towards collaboration—such as those in this report—need stronger commitment. Since consensus on AI policy will require specific and actionable proposals that account for the nuances of AI and its broad application, we are encouraged to continue this work and dive deeper into more specific AI topics affecting international cooperation. Among other potential issues, future discussions will likely cover the EU's AI legislation and its potential global impact, the most promising mechanisms for regulatory alignment, the state and challenges to standards development, and the response to authoritarian use and dissemination of AI, especially by China.

4.1. Preliminary policy recommendations

Below, we present recommendations for developing international cooperation on AI based on our discussions and work to date. For each recommendation, we provide a brief rationale, indicate the level of cooperation that we would consider optimal (on an incremental scale that goes from mere exchange of good practices to cooperation, mutual recognition, full alignment or harmonization, and joint action); and state whether we believe the recommendation can be implemented already in the near term, or over a longer timeframe.

R1. Commit to considering international cooperation in drafting and implementing national AI policies

All FCAI governments have explicitly recognized the value of international collaboration on AI policies and development. These governments should build on this recognition with commitments to cooperating with each other and with international partners prior to adopting AI policies and regulations. Canada has already embedded international regulatory cooperation in guidance on regulatory impact analysis.[302] The U.S. took a significant step in that direction by directing federal agencies to develop plans for international engagement as part of their AI strategies.[303] A similar firm commitment to international collaboration would strengthen trust among governments and confidence in the future of international collaboration. Such a commitment should also go beyond a strict reference to AI, to encompass related critical and emerging technologies such as the Internet of Things, platforms, and data policies (as the U.S.-EU Trade & Technology Council does in part).

Such a recommendation could be implemented within a relatively short timeframe and initially would take the form of firm declarations by individual countries along the lines of Canada's. Ultimately this could also lead to a joint declaration with clear commitments in common on the part of the governments involved.

R2. Refine a common approach to responsible AI development

The seven governments in the FCAI have all adopted AI ethical principles—with 2019 a watershed year for public pronouncements. However, there is not universal agreement in these documents. As explained in Section 3 (page 43), principles such as social and environmental sustainability and human oversight are not embraced in the same way by all FCAI governments, even if the distinctions are clearly far fewer than the commonalities. We recommend that FCAI governments continue progress on a common approach to responsible AI. This can be done in the short term, since all FCAI governments have formalized their current approaches and already are working in forums such as GPAI on this specific issue. The FCAI can support this process by providing a platform for comparative analysis of existing principles, as well as their translation into guidance for individual use cases or for sectoral cooperation (see below).

R3. Agree on a common, technology-neutral definition of AI systems

As a step toward enhanced regulatory cooperation as well as cooperation in standards and R&D projects, countries participating in the FCAI should work on a common definition of AI that is technology-neutral and broad. Based on the definitions among FCAI participants and the work under way in the OECD expert groups, converging on a common definition of AI and working together to gradually update the description of an AI system and its possible configurations and techniques appears feasible. As discussed in Section 3 (page 43), a common definition affects the scope of national policies on AI, and therefore can shape the level of ambition that can be reached by international regulatory cooperation.

Agreeing on a common definition may also entail refinement of the definition to be used in future regulatory initiatives, along with examples and use cases that could help clarify how, and to what extent, the definition applies. This recommendation can be implemented in a relatively short term and requires joint action by FCAI governments. The time to act is short, as the rather broad definition given in the EU AI regulation is undergoing the legislative process in the EU and many other countries are still shaping their AI policy frameworks. Reaching agreement on a common definition would be much more difficult and lengthy if these policy frameworks are finalized on the basis of divergent approaches to the definition of AI.

R4. Agree on the contours of a risk-based approach

As discussed, a risk-based approach to AI policy and regulation has been endorsed by several governments, international organizations, and private actors and provides a crucial opportunity for regulatory alignment. Pursuing this opportunity requires deeper understanding of (1) what risks should be considered, (2) whether a risk classification system should be adopted in this context, and (3) what type of risk assessment should be performed with different risk levels. If FCAI governments should adopt similar regulatory frameworks for responsible AI development, cooperation could be pushed further, conceivably encompassing requirements associated with different risk levels and common or converging approaches to auditing AI systems either ex ante or post-deployment.

Alignment by FCAI governments on a risk-based approach to AI would be an important step towards an interoperable system of responsible AI. It would also facilitate cooperation among FCAI governments, industry, and civil society working on AI standards in international SDOs. General agreement on a risk-based approach could be achieved in the short term; developing the contours of a risk-based classification system would probably take more time and require deeper cooperation among FCAI governments as well as stakeholders.

R5. Establish “redlines” in developing and deploying AI

A key element of any risk classification system will be defining uses of AI, or approaches to AI development or deployment, that should be considered incompatible with the legal systems and values of FCAI countries or protection of democratic processes, including most notably basic requirements of security and protection of individual rights. Cooperation among FCAI governments would advance significantly if they agreed on such boundaries and would provide a collective counterpoint to China’s authoritarian use of AI systems to complement the EU’s proposed prohibition on government use of social credit scores or mass surveillance in public spaces

Agreeing on redlines would entail an iterative process, and depends on fundamental alignment on a risk-based approach (R4) as well as the degree of alignment on a common approach to responsible AI development (R2). FCAI governments could agree on an initial, limited list of redlines such as certain AI uses for generalized social scoring by governments; and then gradually expand the list over time to include emerging AI uses on which there is substantial agreement on the need to prohibit use.

R6. Strengthen sectoral cooperation, starting with more developed policy domains

Several governments are focusing AI policy within specific sectors, and the EU's proposed regulation treats sectors subject to existing product safety regimes as high-risk sectors subject to conformity assessment. In many sectors, specialized regulatory agencies may need to adjust their policy portfolios to the challenges and opportunities presented by the diffusion of AI. Regardless of whether countries adopt a horizontal regulatory framework or a more sector-specific one, there will be need for ongoing dialogue and cooperation among cross-cutting regulators (e.g., data protection authorities, AI agencies, cybersecurity authorities) and also among sector-specific ones (e.g., financial regulators and health regulators). The more these institutions align on principles or on risk frameworks, the greater will be the opportunity for sector-specific coordination.

Sectoral cooperation can be organized on relatively short timeframes starting from sectors that have well-developed regulatory systems and present higher risks, such as health care, transport and finance, where adaptation to AI could be achieved relatively swiftly. In some of these sectors, regulators have already produced orientations, guidelines, or even regulatory frameworks on how to adapt sectoral regulation to AI (e.g., autonomous vehicles and medical devices). This could also be combined with cooperation on sandboxes (R7) and data governance (R10).

R7. Create a joint platform for regulatory learning and experiments

Many FCAI governments are likely to engage in experimental regulation over the coming months. Policy learning would be significantly promoted if FCAI participants set up a joint platform for reporting learning from AI uses cases. Several countries and specialized regulatory bodies have set up "regulatory sandboxes" designed to enable experimentation in areas of legal uncertainty (or, in the case of the EU's proposed AI regulation, to test compliance). Given the complexity and the resource-intensiveness of regulatory sandboxes, it would be useful if FCAI governments could cooperate and even join forces in testing the compliance of specific AI applications with principles of responsible AI development. Indeed, principles and best practices on how to run sandboxes are still missing at the international level, even if international organization such as the OECD have been working on the issue, and some FCAI governments have advanced in the production of guidelines in specific domains (e.g., autonomous vehicles).[304]

A joint repository of regulatory sandboxes could also stimulate dialogue on how to design and implement sandboxes and secure sound governance, transparency, and reproducibility of results, and aid their transferability across jurisdictions and categories of users. Such an information-sharing platform is similar to the role the OECD plays today as an Artificial Intelligence Policy Observatory and the secretariat for GPAI and in convening members and others to monitor AI policy development and practices. That role could be enlarged and systematized to monitor several key aspects of

international policy developments and practices. In turn, GPAI and other multilateral and bilateral cooperation channels should encompass exchange of information in these areas.

This exercise would be useful even in the absence of convergence on the policy framework, but the benefits would be even greater to the extent there is convergence on principles and approach to AI risks. This recommended action is independent of others and is feasible in the short term. It requires soft cooperation, in the form of a structured exchange of good practices. Over time, the repository should become richer in terms of content, and therefore more useful, especially if information and resources are stored in ways that makes them easily retrievable.

R8. Step up cooperation and exchange of practices on the use of AI in government

Government procurement of AI systems is an area where governments have important influence on AI marketplaces and need rules in place that are consistent with their policies and values. As discussed in Section 2 (page 26), development of policies in this area has been a common element of FCAI governments' activity on AI.

These and other governments can leverage their procurement roles by acting collectively: They could set up, either as a stand-alone initiative or in the context of a broader framework for cooperation, a structured exchange on government uses of AI. The dialogue may involve AI applications to improve the functioning of public administration such as the administration of public benefits or health care; AI-enabled regulation and regulatory governance practices; or other decisionmaking and standards and procedures for AI procurement. (Uses of AI in the context of weapons systems is a separate track). Sharing best practices and agreeing on common requirements to government procurement and auditing for AI would also reduce barriers for AI deployers to access a broad international market as well as drive industry practices across this global market with a consequent increase in competition and quality.

This recommended action could also draw on existing initiatives, such as the European Commission Joint Research Centre's "AI Watch" report in the European Union and the U.K. government's Guidelines for AI procurement. The action could be implemented already in the short term, although collecting all experiences and setting the stage for further cooperation would require more time.

R9. Step up cooperation on accountability

The diffusion of AI in many markets and economic sectors will present policymakers around the world with challenges to monitor a constantly evolving market. Depending on the extent to which future policy frameworks will converge and the direction of these frameworks, FCAI governments could profit from enhanced cooperation on accountability, whether through

market oversight and enforcement, auditing requirements, or otherwise. This could combine with sectoral cooperation and possibly also with standards development for auditing AI systems.

R10. Assess the impact of AI on international data governance

As outlined in Section 3.2.1 (page 61), data governance and data protection are being discussed in bilateral and multilateral forums. While data governance issues raise issues that are broader than just AI, the importance of data for AI means that AI cooperation mechanisms will also need to address issues around access to and use of data.

First, there is a need for a common understanding of how data governance rules affect AI R&D in areas such as health research and other scientific research, and whether they inhibit the exploration that is an essential part of both scientific discovery and machine learning. Correspondingly, there is need for a critical look at research and development methods to develop a deeper understanding of appropriate boundaries on use of personal data or other protected information. These subjects need to be part of the agenda for the international AI cooperation mechanisms, exchanges, and information repositories discussed above. FCAI will explore these with participants.

In turn, there is also a need to expand the ability the share data on an international basis. An exchange among FCAI government and others on obstacles to sharing data would help to enable such sharing. The exchange should prioritize datasets for sharing and focus on technical obstacles to interoperability of these datasets and opportunities for privacy preserving computation. In addition, FCAI governments should include PPCs in their R&D budgets for AI, and this area could be fertile ground for the joint R&D projects proposed below (R17). Regardless of whether this is done jointly, coordination of funding among FCAI governments is likely to increase the impact.

R11. Adopt a stepwise, inclusive approach to international AI standardization

A stepwise approach to standards development is needed to allow time for technology development and experimentation and to gather the data and use cases to support robust standards. Such a stepwise approach would ensure that discussions at the international level take place once technology has reached a certain level of maturity or where a regulatory environment is adopted. It should start with foundational standards such as a common language and definitions can provide a common basis for application-specific AI solutions. This will include horizontal cross-cutting standards, particularly when it comes to foundational issues such as terminology and reference architecture, risk management, and standards that guide management practices as they relate to AI development and use.[305]

To support a stepwise approach to AI standards, it would be helpful to establish a database of AI standards under development at both national and international levels. Such a database would improve understanding of the landscape of AI developments and support cooperation and coordination where desirable on AI standards development. FCAI governments should also

expand funding that enables universities and SMEs to become increasingly engaged in the technical work needed to support the development of foundational international AI standards.

R12. Develop a coordinated approach to AI standards development that encourages Chinese participation consistent with an industry-led, research-driven approach

FCAI participants need to develop a joint understanding of the opportunities and challenges that China presents to the development of international AI Standards. Governments will likely need to take the lead here, but it must be a multistakeholder process. There is currently a risk of disconnect between growing concern among governments and national security officials alarmed by Chinese engagement in the standards process, on the one hand, and industry participants' perceptions of the impact of Chinese participation in SDOs on the other; at least anecdotally, some Chinese participants are reported to have made useful contributions to SDOs and efforts by China to push China-centric standards that lack technical credibility have not progressed in the key SDOs working on AI such as the ISO, IEC, and IEEE.

To encourage constructive involvement and discourage self-serving standards, FCAI participants (and likeminded countries) should encourage Chinese engagement in international standards setting while also agreeing on costs for actions that use SDOs strategically to slow down or stall standards making. This can be accomplished through trade and other measures but will require cooperation among FCAI participants to be effective.

R13. Expand trade rules for AI standards

There are various ways trade policy can play a more central role in supporting AI standards. This will be a subject of future AI dialogues and the following outlines two areas for further consideration.[306] As noted, the application of international standards to rules in the WTO Technical Barriers to Trade (TBT) Agreement and free trade agreements is limited to goods only, whereas AI standards will apply mainly to services. New trade rules are needed that extend to services, the types of commitments to international standards found in the TBT. As a starting point such rules should be developed in the context of free trade agreements, with the aim to make them multilateral in the WTO. Trade rules are also needed to support data free flow with trust and to reduce barriers and costs to AI infrastructure. Consideration also should be given to linking participation in the development of AI standards in bodies such as ISO/IEC, with broader trade policy goals and compliance with core WTO commitments.

R14. Increase funding for participation in SDOs

Increase funding for academics and industry participation (including SMEs), as well as for meeting in both FCAI countries and less developed countries. Broadened participation is important to democratize the standards-development process and strengthen the legitimacy and adoption of the resulting standards. Increased funding can expand opportunities and speed up standards development as academics and others can help develop draft

standards. Hosting meetings of standards bodies in additional countries can broaden exposure to standards-setting processes around AI and critical technology. Currently, the Chinese government provides funding for attendance at meetings held in China.

R15. Develop common criteria and governance arrangements for international large-scale R&D projects

Joint research and development applying to large-scale global problems such as climate change or disease prevention and treatment can have two valuable effects: It can bring additional resources to the solution of pressing global challenges, and the collaboration can help to find common ground in addressing differences in approaches to AI. FCAI will seek to incubate a concrete roadmap on such R&D for adoption by FCAI participants as well as other governments and international organizations.

This roadmap will involve refining proposed criteria for such R&D projects and move from there to subjects for proposed the projects. Our recommendation in this regard is independent of others; indeed, using collaboration on R&D as a mechanism to work through matters that affect international cooperation on AI policy means that this recommendation should play out in the near term.

4.2. Next steps: Proposed future topics for FCAI dialogues

The recommended actions outlined in the previous section will be subject to consultation with FCAI participants, including government representatives, academics, industry, and civil society, and will then become a basis for structuring the next steps of the FCAI. In particular, we see the following areas as particularly suitable for dialogues in the coming months, and Table 4 illustrates the relationships among these topics and the recommendations above:

- **Scaling R&D cooperation on AI projects.** This dialogue would be aimed at refining the choice of the key requirements for joint R&D projects, as well as the identification of candidates for pilot projects to be launched in the short term. These projects can be both related to specific advancements in AI (e.g., federated learning and other possible ways to reconcile data-hungry techniques with privacy protection); and advances made possible by AI (e.g., AI-enabled solutions for climate change or to detect and respond to future pandemics).

- **China and AI: What are the risks, opportunities, and ways forward?** To what extent, and at what cost, is cooperation with China possible? And what is the cost of not engaging with China, especially in terms of future developments in the global AI market and the possible forking of the technology stack? Where are the pressure points, and where are the possible deal-breakers in the quest for global standards and redlines in the deployment of AI?

- **Government use of AI: Developing common approaches.** What is the current experience with using AI in government, both in terms of back office and citizen-facing applications? What are the key areas for cooperation among FCAI governments in this domain? Can cooperation lead to standards in public procurement of AI systems? What safeguards should be deployed to ensure that no citizen is excluded as a result of government AI deployment?

- **Regulatory cooperation and harmonization:** issues and mechanisms. What are the available options for international regulatory cooperation? What does experience suggest in terms of the preconditions for each of them to be implemented effectively? How to build an incremental path from softer to more structured forms of collaboration? This meeting could also explore possible patterns of harmonization or mutual recognition between legal and regulatory frameworks in FCAI countries.

- **The impact of data governance on AI.** Many countries are introducing national data strategies. Approaches to both personal data and non-personal (industrial) data affect access to data for R&D and the flow of data across borders. This meeting will explore the directions taken in different countries, and how they affect AI R&D and an effective international framework for the free flow of data with trust and privacy.

- **Standards development.** Building on many of the recommendations above, FCAI will continue with dialogues on AI standards development aimed at supporting international cooperation toward global AI standards, minimizing strategic use of SDOs that undermines the industry led nature, and supporting participation by a broad range of actors, including from countries outside FCAI and in the developing world.

- **An AI trade agreement: Partners, content, and strategy.** This dialogue could start from the existing bilateral trade cooperation in the domain of AI (including in the context of the U.S.-EU Trade and Technology Council) to explore possible future mini- or multilateral trade agreements on AI.

Table 4. Aligning policy recommendations with a future path for FCAI dialogues

Topics for future FCAI dialogues	Recommendations
Scaling R&D cooperation on AI projects Refine the scope of joint R&D AI projects, requirements, and candidates for pilot projects.	R1. Commit to considering international cooperation in drafting and implementing national AI policies R3. Agree on a common, technology-neutral definition of AI systems R5. Establish "redlines" in developing and deploying AI R7. Create a joint platform for regulatory learning and experiments R9. Step up cooperation on accountability R15. Develop common criteria and governance arrangements for international large-scale R&D projects
China and AI: What are the risks, opportunities, and ways forward? Gauge the potential extent—and cost—of cooperation with China in future AI issues.	R1. Commit to considering international cooperation in drafting and implementing national AI policies R9. Step up cooperation on accountability R10. Assess the impact of AI on international data governance R12. Develop a coordinated approach to AI standards development that encourages Chinese participation consistent with an industry-led, research-driven approach
Government use of AI: Developing common approaches Discuss experience with deploying AI in the public sector to identify key areas for inter-governmental cooperation—such as safeguards to prevent exclusion of citizens and best practices for public procurement of AI systems.	R1. Commit to considering international cooperation in drafting and implementing national AI policies R2. Refine a common approach to responsible AI development. R3. Agree on a common, technology-neutral definition of AI systems R4. Agree on the contours of a risk-based approach R5. Establish "redlines" in developing and deploying AI R8. Step up cooperation and exchange of practices on the use of AI in government R9. Step up cooperation on accountability R10. Assess the impact of AI on international data governance
Regulatory cooperation and harmonization: Issues and mechanisms Address options for international regulatory cooperation, including structured collaboration and harmonization of legal and regulatory frameworks.	R1. Commit to considering international cooperation in drafting and implementing national AI policies R2. Refine a common approach to responsible AI development R3. Agree on a common, technology-neutral definition of AI systems R4. Agree on the contours of a risk-based approach R5. Establish "redlines" in developing and deploying AI R6. Strengthen sectoral cooperation, starting with more developed policy domains R9. Step up cooperation on accountability

Topics for future FCAI dialogues	Recommendations
A suitable international framework for data governance Further explore national data strategies, their impact on AI R&D, and pathways for an effective international framework for free flow of data with trust and privacy.	R1. Commit to considering international cooperation in drafting and implementing national AI policies R3. Agree on a common, technology-neutral definition of AI systems R2. Refine a common approach to responsible AI development R4. Agree on the contours of a risk-based approach R5. Establish "redlines" in developing and deploying AI R6. Strengthen sectoral cooperation, starting with more developed policy domains R9. Step up cooperation on accountability R10. Assess the impact of AI on international data governance R15. Develop common criteria and governance arrangements for international large-scale R&D projects
Standards development Map cooperation toward global AI standards, minimizing strategic use of SDOs to undermine the technically-driven standards development, and broaden participation by stakeholders outside FCAI and in the developing world.	R1. Commit to considering international cooperation in drafting and implementing national AI policies R3. Agree on a common, technology-neutral definition of AI systems R11. Adopt a stepwise, inclusive approach to international AI standardization R12. Analyze additional AI standards needed and establish information-sharing networks R12. Develop a coordinated approach to AI standards development that encourages Chinese participation consistent with an industry-led, research-driven approach R13. Expand trade rules for AI standards R14. Increase funding for participation in SDOs
An AI trade agreement: Partners, content, and strategy Build on existing bilateral trade cooperation in the domain of AI—plurilateral or multilateral trade agreements on AI.	R1. Commit to considering international cooperation in drafting and implementing national AI policies R3. Agree on a common, technology-neutral definition of AI systems R6. Strengthen sectoral cooperation, starting with more developed policy domains. R10. Assess the impact of AI on international data governance R13. Expand trade rules for AI standards

	FUTURE FCAI DIALOGUE TOPICS						
	Scaling up cooperation on AI projects	China and AI: Risks, opportunities, and, ways forward?	Government use of AI: Developing common approaches	Regulatory cooperation and harmonization: Issues and mechanisms	A suitable international framework for data governance	Standards development	Trade agreements: Partners, content, and strategy
R1. Commitment to international cooperation when drafting and implementing national AI policies	✓	✓	✓	✓	✓	✓	✓
R2. A common approach to responsible AI development	✓	✓	✓	✓		✓	✓
R3. A common definition of AI systems for both technical and regulatory purposes			✓	✓		✓	
R4. Gradual alignment of risk-based approaches	✓		✓	✓			✓
R5. Convergence on "redlines", or prohibited AI applications		✓		✓			
R6. Sectoral cooperation	✓		✓	✓		✓	✓
R7. A platform for joint learning, experiments	✓			✓		✓	✓
R8. Cooperation on government use of AI			✓	✓			✓
R9. Common accountability principles practices		✓		✓		✓	✓
R10. Strengthen international data governance to support AI development and uptake	✓		✓	✓	✓	✓	✓
R11. An inclusive approach to international AI standards		✓	✓		✓	✓	✓
R12. A coordinated approach to standards development that encourages constructive Chinese participation		✓					
R13. Expanded trade rules for AI standards		✓	✓	✓	✓	✓	✓
R14. Increased funding for participation in SDOs		✓				✓	
R15. Develop selection criteria and governance for international large-scale R&D projects	✓						

ANNEX 1.

AI POLICIES AND INVESTMENT BY FCAI PARTICIPANTS

	AI ethical framework[307]	Existing AI regulation[308]	Data governance[309]			AI Standards[310]	Computing power
			Privacy	IP	Cyber		
AU[311]	Australia's Ethics Framework	Review of existing regulations per the AI Action Plan	Privacy Act; Australian Privacy Principles (APPs)	IP Government Open Data Government Open Data	Security of Critical Infrastructure Act	Standards Australia focuses on by-design and standards testing; Australia's AI Standards Roadmap	Envisage new offices on key critical technology areas (quantum, biotechnology, and AI)
CA[312]	CIFAR Pan-Canadian AI Strategy 2017; Canada's Digital Charter 2017, updated 2021; Government of Canada's Advisory Council on AI (Public Awareness Working Group); Montreal Declaration for Responsible Development of AI	Directive on Automated Decision Making; Algorithmic Impact Assessment (governmental); Bill C-11 (tabled)	Personal Information Protection/ Electronic Documents Act 2011 (PIPEDA); Consumer Privacy Protection Act proposed in the Digital Charter Implementation Act 2020, which modifies PIPEDA; Provincial privacy legislation	Copyright Act; IP Strategy	No federal legislation, parts of PIPEDA; Emergencies Act; Criminal Code S. 342.1 and 430; Canada Anti-Spam Legislation; National Cyber Security Strategy (2019) (announced)	CIO Strategy Council develops AI Standards and is accredited by Sandards Council of Canada, focusing on ethical design and ADM audits; $8.6 million over five years, starting in 2021–22, to advance the development and adoption of AI standards	$360 million for Quantum Research in Budget 2021, ranking 5th in the G-7 in total, expenditure on quantum science (1st per capita)
EU[313]	Ethics Guidelines for Trustworthy AI; Proposal for a regulation on AI; White Paper on AI; national ethics guidelines	Coordinated Plan on AI; AI Act (proposed); Digital Decade package	GDPR; Payment Services Directives (PSD 1 / PSD 2); eIDAS Regulation	EU copyright law (11 directives, two regulations)	Cybersecurity Act; NIS Directive	CEN-CENELC Joint Technical Committee 21 'Artificial Intelligence'; national standards focus on EU interoperability, ethics, fundamental rights, and safety	7 billion euros for EU High Performance Computing Joint Undertaking (EuroHPC JU); Digital Innovation Hubs
JA[314]	R&D Guidelines 2018; Social Principles of Human-Centric AI 2019; AI Utilization Guidelines 2019; Society 5.0 framework	Draft AI Utilization Principles Guidelines 2019; AI Technology Strategy 2017	Protection of Personal Information (APPI); Data Free Flow with Trust (DFFT)	Unfair Competition Prevention Act; Patent rights, utility model rights, design rights, trademark rights, and copyrights	Partial revision to the Criminal Code (Cyber Criminal Code); Act on the Prohibition of Unauthorised Computer Access 2012; Basic Act on Cybersecurity 2014	Ministry of Economy, Trade and Industry (METI), Japanese Industrial Standards Committee and Information Technology Standards Commission focus on developing sector-specific standards in transportation, safety, and patents	Supercomputer ranked 1st worldwide (Fugaku, Kobe); AI Bridging Cloud Infrastructure (ABCI)

	AI ethical framework[307]	Existing AI regulation[308]	Data governance[309]			AI Standards[310]	Computing power
			Privacy	IP	Cyber		
SI[315]	Model AI Governance Framework, 2nd Edition, 2020; Implementation and Self-Assessment Guide for Organisations (ISAGO); Principles to Promote Fairness, Ethics, Accountability and Transparency (FEAT)	National AI Strategy	Personal Data Protection Act 2012 (PDPA) (amended in 2020); Trusted Data Sharing Framework (voluntary)	Patents Act; Copyright Act; AI2 Scheme for fast-track examination	Cybersecurity Act 2018; Computer Misuse Act	Spring SG: Voluntary Horizontal Model Framework also contributes to global standards for AI-related policies and guidelines	NSCC cooperates with Japan's RIKEN and RIST to access Fugaku; National Research Foundation builds second national supercomputer system (SG$200 million)
U.K.[316]	Guidance on Ethics, Transparency Accountability for ADM	National AI Strategy	Data Protection Act 2018 (U.K. GDPR); U.K. eIDAS Regulation	Copyright, Designs and Patents Act 1988	Cyber Security Information Sharing Partnership, UK GDPR	British Standard Institute focuses on international cooperation and healthcare standards	GBP 20 million funding for DiRAC (academic); High Performance Computing facility
US[317]	Principles in Executive Order 13859 and Executive Order 13960; Agency specific frameworks, state-specific guidelines	Government agencies assessing where AI regulation is needed, where existing regulation applies, and roles for self assessment, codes, etc.	Vertical federal privacy regulation e.g., health, children, and state-specific privacy bills (CCPA)	Patents or U.S. copyright law	State-specific	National Institute of Standards and Technology (NIST) and American National Standards Institute (ANSI) focus on maintaining U.S. leadership/ priority, international engagement, foundational AI standards	National supercomputers (private and public) ranked 2nd, 3rd, 5th, 9th worldwide National Quantum Initiative Act with $2.2bn funding

	Public Investment[318]	Private Investment[319]	R&D (private and/or public)[320]	Programs
AU	AUD $124.1 million (USD 90.9 million) 2021-2022	No data available	No data available	2021 AI Action Plan
CA	CAD 125 million (USD 100 million) 2017-2022	USD $314 (2019)	CAD 900 million (710 million USD) 2017-2021 (foreign direct investment), CAD 1 billion (USD 789 million) (public)	CIFAR Pan-Canadian AI Strategy
EU	EUR 20 billion (USD 23.3 billion) per year until 2030, national funding	USD $2044 (2020)	EUR 1.5 billion (USD 1.75 billion) 2018-2020 (public), national funding	Horizon 2020, Horizon Europe, Recovery and Resilience Facility, national funding
JA	Yen 77 billion (USD 70 billion) 2018	USD $510 (2019)	Yen 600 billion (USD 546 billion) 2018	AI Strategy 2019
SI	Up to SG$150 million (USD 110.8 million) 2017-2022	USD $314 (2019)	S$500 million (USD 369 million) 2016-2020 (public)	National AI Strategy, AI Singapore program, Research, Innovation and Enterprise 2020 Plan
U.K.	GBP 1 billion (USD 1.36 billion) 2018-2027	USD $1,655 (2019)	GBP 4.7 billion (USD 6.6 billion) 2018-2022 (public)	AI Sector Deal, Industrial Strategy Challenge Fund, U.K. Digital Strategy
US	USD 1.9 billion (2018-2020)	USD $25,170 (2019)	USD 6 billion 2021 (public)	American AI Initiative and FY 2021 budget, annual reports, supplementary documents

These tables include non-exhaustive examples and estimates drawn from external sources and the authors' own analysis, and are not a complete representation of investment or research and development totals.

ANNEX 2.

MODE OF OPERATION, MEMBERSHIP, AND VOTING PROCEDURES OF SELECTED SDOS

SDO	Operation	Membership	Voting Procedures
International Electrotechnical Commission (IEC)	» Nonprofit, quasi-governmental international organization	» Composed of one national committee per country, which appoints experts and delegates from industry, government bodies, associations, and academia to participate in the work of the IEC.	» 62 full voting members » 27 associate members with limited voting rights in » Standard approvals are finalized if two-thirds of members vote to approve, and if less than 25 percent of all submitted votes are negative.[321][7][1]
Institute of Electrical and Electronics Engineers (IEEE)	» Nonprofit, technical professional association » IEEE Standards Association (IEEE SA) is the standards setting body within the IEEE	» IEEE SA working groups are open groups comprised of individuals for individual standards projects, while corporate standards projects are comprised of representatives from corporations, government agencies, or academic institutions.	» Although anyone can join IEEE SA working groups, payment of an IEEE or IEEE SA membership fee or of a per-ballot fee is required to vote on standards. » An IEEE SA standard will pass the balloting process if at least 75 percent of all ballots from a balloting group are returned, and if 75 percent of these bear a "yes" vote. If ballot returns of 30 percent are abstentions, the ballot fails.[322][8][2] The IEEE SA Standards Board approves or disapproves standards that have passed the ballot process based on the recommendation of its Standards Review Committee (RevCom).[323][9]
International Organization for Standardization (ISO)	» Quasi-governmental international organization » Global network of national standard setting bodies	» Full members (member bodies) participate and vote in ISO technical and policy meetings. » Correspondent members attend ISO technical and policy meetings as observers and have no voting rights. » Subscriber members take notice of the ISO's work but do not participate in it.	» The ISO applies the principle of "one country, one vote," with votes cast by ISO member bodies.
International Telecommunication Union Telecommunication Standardization Sector (ITU-T)	» The ITU is the U.N. specialized agency for information and communication technologies (ICTs).[324][10] ITU-T develops standards through multistakeholder study groups.[325][11][5]	» Sector member: Can access all ITU-T study groups and the full range of ITU-T activities. » Associate: Can participate in one chosen study group. » Academia: Can access all ITU-T study groups.[326][12][6]	» Participants from all membership categories can contribute to the standards making process, but only Sector members have the right to participate in final decisionmaking.[327][13] » Standards approval primarily facilitated by the Alternative Approval Process (AAP)[328][14]

ENDNOTES

1. Daniel Zhang, et al., "The AI Index 2021 Annual Report," AI Index Steering Committee, Human-Centered AI Institute, Stanford University, March 2021, https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report_Master.pdf.
2. Brenda Leong, "The spectrum of artificial intelligence—an infographic tool," Future of Privacy Forum, December 14, 2020, https://fpf.org/blog/the-spectrum-of-artificial-intelligence-an-infographic-tool/.
3. Jacques Bughin, et al., "Notes from the AI frontier: Modeling the impact of AI on the world economy," McKinsey Global Institute, September 4, 2018, https://www.mckinsey.com/featured-insights/artificial-intelligence/notes-from-the-ai-frontier-modeling-the-impact-of-ai-on-the-world-economy.
4. "OECD AI policy observatory," OECD, accessed August 25, 2021, https://www.oecd.ai/.
5. Section 2 below summarizes the main developments in the seven administrations, with specific focuses on AI strategies and policies.
6. The Global Partnership on Artificial Intelligence, accessed August 25, 2021, https://www.gpai.ai/community/.
7. Data from "GDP (current US$)," World Bank, accessed May 1, 2021, https://data.worldbank.org/indicator/NY.GDP.MKTP.CD.
8. Jeffrey L. Furman and Patrick Gaule, "A review of economic perspectives on collaboration in science," National Research Council, Study of the Science of Team Science, updated October 22, 2013, https://sites.nationalacademies.org/cs/groups/dbassesite/documents/webpage/dbasse_085533.pdf.
9. Hanna Hottenrott and Cindy Lopes-Bento, "R&D partnerships and innovation performance: Can there be too much of a good thing?" Dusseldorf Institute for Competition Economics, July 2014, https://d-nb.info/1054730210/34.
10. Knut Blind, Andre Jungmittag, and Axel Mangelsdorf, "The economic benefits of standardisation. An update of the study carried out by DIN in 2000," DIN Deutsches Institut fur Normung e.V., January 2021, https://www.researchgate.net/publication/255869222_The_economic_benefits_of_standardisation_An_update_of_the_study_carried_out_by_DIN_in_2000.
11. "International regulatory co-operation: Addressing global challenges," OECD Publishing, April 24, 2013, http://dx.doi.org/10.1787/9789264200463-en; "International regulatory co-operation: The role of international organisations," OECD Publishing, November 3, 2014, http://dx.doi.org/10.1787/9789264225756-en.
12. Duncan Snidal, "The limits of hegemonic stability theory," *International Organization, V*ol. 39, Issue 4, 1985, https://www.cambridge.org/core/journals/international-organization/article/abs/limits-of-hegemonic-stability-theory/8E5D4F10ABA32BE7545EFBBC84EA7BFB; Kenneth W. Abbott and Duncan Snidal, "Why states act through formal international organizations," *The Journal of Conflict Resolution*, Vol. 42, No. 1, February 1998), https://www.jstor.org/stable/174551; Bernard M. Hoekman, "International regulatory cooperation in a supply chain world," in *Redesigning Canadian trade policies for new global realities,* ed. Stephen Tapp, Ari Van Assche, and Robert Wolfe (Ottawa : Institute on Research on Public Policy, 2015,, p. 1–29, https://cadmus.eui.eu//handle/1814/39090.
13. Haotian Hu, Dongbo Wang, and Sanhong Deng, "Global collaboration in artificial intelligence: Bibliometrics and network analysis from 1985 to 2019," *Journal of Data and Information Science*, Vol. 5 Issue 4, September 2020, https://www.researchgate.net/publication/347517300_Global_Collaboration_in_Artificial_Intelligence_Bibliometrics_and_Network_Analysis_from_1985_to_2019.
14. Sarah O'Meara, "AI researchers in China want to keep the global-sharing culture alive," *Nature,* May 29, 2019, https://www.nature.com/articles/d41586-019-01681-x.
15. OECD, "The State of Implementation of the OECD AI Principles," (June 18, 2021),https://www.oecd.org/digital/state-of-implementation-of-the-oecd-ai-principles-1cd40c44-en.htm, visualizations powered by Josef Stefan Institute using data from Microsoft Academic Graph version of 12/1/2/2020, accessed 4/3/2021.
16. A good example is the U.S. Administration's decision to launch an initiative aiming to make more government data available to AI researchers as part of a broader push to keep the U.S. on the cutting edge of the crucial new technology. See Ryan Tracy, "U.S. launches task force to study opening government data for AI research," *The Wall Street Journal,* June 10, 2021, https://www.wsj.com/articles/u-s-launches-task-force-to-open-government-data-for-ai-research-11623344400.
17. See e.g., Bertin Martens, "The impact of data access regimes on artificial intelligence and machine learning," JRC Digital Economy Working Paper 2018–19, EU Science Hub, https://ec.europa.eu/jrc/en/publication/eur-scientific-and-technical-research-reports/impact-data-access-regimes-artificial-intelligence-and-machine-learning.
18. Saurabh Mishra and Keith Strier, "Computing to win: Addressing the policy blind spot that threatens national AI ambitions," *The Atlantic*

Council, New Atlanticist, April 29, 2021, www.atlanticcouncil.org/blogs/new-atlanticist/computing-to-win-addressing-the-policy-blind-spot-that-threatens-national-ai-ambitions/.

19. Dario Amodei and Danny Hernandez, "AI and compute," *OpenAI,* May 16, 2018, https://openai.com/blog/ai-and-compute/.
20. Or Sharir, Barak Peleg, and Yoav Shoham, "The cost of training NLP models: A concise overview," AI21 Labs, April 2020, https://arxiv.org/pdf/2004.08900.pdf
21. Alec Radford, et al., "Better language models and their implications," OpenAI, February 14, 2019, https://openai.com/blog/better-language-models/; Karen Simonyan and Andrew Zisserman, "Very deep convolutional networks for large-scale image recognition," ICLR, 2015, https://arxiv.org/pdf/1409.1556.pdf; Christian Szegedy et al., "Inception-v3," accessed September 1, 2021, https://paperswithcode.com/method/inception-v3.
22. Daniel Zhang, et al., "The AI Index 2021 Annual Report," AI Index Steering Committee, Human-Centered AI Institute, Stanford University, March 2021, https://aiindex.stanford.edu/wp-content/uploads/2021/03/2021-AI-Index-Report_Master.pdf.
23. That said, as China's progress on AI is seen as a national security and economic risk, the engagement of China in international collaboration on AI R&D is under scrutiny, particularly where the hand of the Chinese government is seen. This includes greater attention to whether Chinese AI researchers are being funded by the government or its security apparatus, and how the government can access the AI insights that its researchers gain while working internationally.
24. "Recommendation of the Council on artificial intelligence," OECD Legal Instruments, May 21, 2019, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.
25. "OECD to host Secretariat of new Global Partnership on Artificial Intelligence," OECD, June 15, 2020, https://www.oecd.org/going-digital/ai/oecd-to-host-secretariat-of-new-global-partnership-on-artificial-intelligence.htm.
26. "AI ethics guidelines global inventory," *AlgorithmWatch,* accessed August 25, 2021, https://inventory.algorithmwatch.org/.
27. "AI initiatives," Council of Europe Portal, accessed August 25, 2021, https://www.coe.int/en/web/artificial-intelligence/national-initiatives.
28. "Asilomar AI principles," Future of Life Institute, 2017, https://futureoflife.org/ai-principles/.
29. The IEEE currently operates under its acronym. It was formerly known by its long form name, the Institute of Electrical and Electronics Engineers. Also see: "Ethically aligned design: A vision for prioritizing human well-being with autonomous and intelligent systems," IEEE, 2019, https://standards.ieee.org/content/dam/ieee-standards/standards/web/documents/other/ead1e.pdf?utm_medium=undefined&utm_source=undefined&utm_campaign=undefined&utm_content=undefined&utm_term=undefined.
30. Meredith Whittaker, et al., "AI Now report 2018," New York University, AI Now Institute, December 2018, https://ainowinstitute.org/AI_Now_2018_Report.pdf.
31. Thilo Hagendorff, "The ethics of AI ethics: An evaluation of guidelines," Minds and Machines, February 1, 2020, https://doi.org/10.1007/s11023-020-09517-8.
32. Anna Jobin, Marcello Lenca, and Effy Vayena, "The global landscape of AI ethics guidelines," *Nature Machine Intelligence,* September 2, 2019, https://www.nature.com/articles/s42256-019-0088-2.
33. Thierry Breton, "European companies must be ones profiting from European data," *POLITICO*, January 19, 2020, https://www.politico.eu/article/thierry-breton-european-companies-must-be-ones-profiting-from-european-data/.
34. "Regulatory divergence: Costs, risks, impacts," IFAC and BIAC, April 11, 2018, https://www.ifac.org/knowledge-gateway/contributing-global-economy/publications/regulatory-divergence-costs-risks-and-impacts.
35. Nick Kostov and Sam Schechner, "GDPR has been a boon for Google and Facebook," *The Wall Street Journal,* June 17, 2019, https://www.wsj.com/articles/gdpr-has-been-a-boon-for-google-and-facebook-11560789219.
36. "Regulatory divergence: costs, risks, impacts," International Federation of Accountants, February 2018, https://www.ifac.org/system/files/publications/files/IFAC-OECD-Regulatory-Divergence.pdf.
37. Joshua P. Meltzer, "Artificial intelligence primer: What is needed to maximize AI's economic, social, and trade opportunities," The Brookings Institution, Global Views, No. 12, May 2019, https://www.brookings.edu/wp-content/uploads/2019/05/ai-primer_global-view_final.pdf; Avi Goldfarb and Daniel Trefler, "AI and international trade," NBER Working Paper 24254, January 2018, https://www.nber.org/papers/w24254.
38. Peter Gailhofer, et al., "The role of artificial intelligence in the European Green Deal," European Parliament, May 2021, https://www.europarl.europa.eu/RegData/etudes/STUD/2021/662906/IPOL_STU(2021)662906_EN.pdf; Ricardo Vinuesa, Hossein Azizpour, et al., "The role of artificial intelligence in achieving the Sustainable Development Goals," *Nature Communications,* January 13, 2020, https://doi.org/10.1038/s41467-019-14108-y.
39. "Artificial intelligence in road traffic crash prevention roundtable," International Transport Forum, February 10-12, 2021, https://www.itf-oecd.org/artificial-intelligence-crash-prevention-roundtable; "Artificial intelligence in the delivery of public services," United Nations Economic and Social Commission for Asia and the Pacific and Google, https://www.unescap.org/sites/default/d8files/knowledge-products/AI%20Report.pdf; "Anna Schneider-Kamp, "The potential of AI in care optimization: insights from the user-driven co-development of a care integration system," Inquiry: A Journal of Medical Care Organization, Provision and Financing, May 24, 2021, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC8150466/.
40. "Drones use machine learning to detect landmines," Tech Briefs, July 1, 2021, ; "Project AIMS (Artificial Intelligence against Modern Slavery," The Future Society, March 17, 2021, https://thefuturesociety.org/2021/03/17/project-aims-artificial-intelligence-against-modern-slavery/.

41. Fu Ying and John Allen, "Together, the U.S. And China can reduce the risks from AI", Noema, December 17, 2020, https://www.noemamag.com/together-the-u-s-and-china-can-reduce-the-risks-from-ai/.

42. Adrian Shahbaz, "The rise of digital authoritarianism," Freedom House, October 2018, https://freedomhouse.org/report/freedom-net/2018/rise-digital-authoritarianism.

43. Gregory C. Allen, "Understanding China's AI strategy: Clues to Chinese strategic thinking on artificial intelligence and national security," Center for a New American Security, February 6, 2019, https://www.cnas.org/publications/reports/understanding-chinas-ai-strategy?utm_medium=email&utm_campaign=Understanding%20Chinas%20AI%20Strategy%20White%20Paper%20Rollout%20Media&utm_content=Understanding%20Chinas%20AI%20Strategy%20White%20Paper%20Rollout%20Media+CID_eecdd0d32a84c74e153b8409074cd04e&utm_source=Campaign%20Monitor&utm_term=Read%20the%20full%20paper.

44. Kieron O'Hara, Wendy Hall, "Four internets: The geopolitics of digital governance," CIGI Papers Series, December 7, 2018, https://www.cigionline.org/publications/four-internets-geopolitics-digital-governance.

45. Will Knight, "Why does Beijing suddenly care about AI ethics?" MIT Technology Review, May 31, 2019, https://www.technologyreview.com/2019/05/31/135129/why-does-china-suddenly-care-about-ai-ethics-and-privacy/.

46. "Artificial intelligence roadmap," Commonwealth Scientific and Industrial Research Organisation (CSIRO), November 2019, https://www.csiro.au/en/research/technology-space/ai/artificial-intelligence-roadmap.

47. "Artificial intelligence," Australia's Digital Economy, May 6, 2021, https://digitaleconomy.pmc.gov.au/fact-sheets/artificial-intelligence.

48. Jordan Cox, Aya Lewih, and Irene Halforty, "AI, machine learning, & big data laws and regulations 2021," Global Legal Insights, 2021, https://www.globallegalinsights.com/practice-areas/ai-machine-learning-and-big-data-laws-and-regulations/australia.

49. "Australia's AI Action Plan," Commonwealth of Australia, June 2021, https://www.industry.gov.au/sites/default/files/June%202021/document/australias-ai-action-plan.pdf.

50. "An artificial intelligence standards roadmap: Making Australia's voice heard," Standards Australia, https://www.standards.org.au/getmedia/ede81912-55a2-4d8e-849f-9844993c3b9d/R_1515-An-Artificial-Intelligence-Standards-Roadmap-soft.pdf.aspx. Adam Stingemore, Angela Williams, and Samantha Smith, "Standards Australia sets priorities for artificial intelligence," Standards Australia, March 12, 2020, https://www.standards.org.au/news/standards-australia-sets-priorities-for-artificial-intelligence.

51. "Australia's AI Action Plan," Commonwealth of Australia, June 2021, https://www.industry.gov.au/sites/default/files/June%202021/document/australias-ai-action-plan.pdf.

52. "Australia's AI Action Plan," Commonwealth of Australia, June 2021, https://www.industry.gov.au/sites/default/files/June%202021/document/australias-ai-action-plan.pdf.

53. "Pan-Canadian AI Strategy," CIFAR, accessed August 25, 2021, https://cifar.ca/ai/.

54. "Budget 2021: A recovery plan for jobs, growth, and resilience," Government of Canada, accessed August 25, 2021, https://www.budget.gc.ca/2021/home-accueil-en.html; Daniel Banks, "2021 federal budget provides new funding for quantum technology, artificial intelligence, clean energy technologies, life sciences, and student internships," Canadian Association of Physicists, April 20, 2021, https://www.cap.ca/publications/cap-news/proposed-2021-federal-budget/#c.

55. "Canada concludes inaugural plenary of the Global Partnership on Artificial Intelligence with international counterparts in Montreal," Markets Insider, December 4, 2020, https://markets.businessinsider.com/news/stocks/canada-concludes-inaugural-plenary-of-the-global-partnership-on-artificial-intelligence-with-international-counterparts-in-montr%C3%A9al-1029866048.

56. "Montreal Declaration for the responsible development of AI," accessed August 25, 2021, https://www.montrealdeclaration-responsibleai.com/the-declaration.

57. "Directive on automated decision-making," Government of Canada, April 1, 2021, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592.

58. "PIPEDA fair information principles," Office of the Privacy Commissioner of Canada, revised May 2019, https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/.

59. "Canada's Digital Charter: Trust in a digital world," Government of Canada, modified January 12, 2021, https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html.

60. The Global Partnership on Artificial Intelligence, accessed August 25, 2021, https://gpai.ai/.

61. "Canada concludes inaugural plenary of the Global Partnership on Artificial Intelligence with international counterparts in Montreal," Markets Insider, December 4, 2020, https://markets.businessinsider.com/news/stocks/canada-concludes-inaugural-plenary-of-the-global-partnership-on-artificial-intelligence-with-international-counterparts-in-montr%C3%A9al-1029866048.

62. "Advisory Council on Artificial Intelligence," Government of Canada, updated July 13, 2021, http://www.ic.gc.ca/eic/site/132.nsf/eng/home; "Terms of reference of the Government of Canada Advisory Council on Artificial Intelligence," Government of Canada, updated May 14, 2019, http://www.ic.gc.ca/eic/site/132.nsf/eng/00003.html.

63. "Canada and the United Kingdom collaborate on responsible artificial intelligence," Government of Canada, February 27, 2020, https://www.canada.ca/en/social-sciences-humanities-research/news/2020/02/canada-and-the-united-kingdom-collaborate-on-responsible-artificial-intelligence.html.

64. "Coordinated Plan on Artificial Intelligence (COM(2018) 795 final)," European Commission, December 7, 2018, https://knowledge4policy.ec.europa.eu/publication/coordinated-plan-artificial-intelligence-com2018-795-final_en.

65. "High-level expert group on artificial intelligence," European Commission, updated June 23, 2021, https://digital-strategy.ec.europa.eu/en/policies/expert-group-ai.
66. "New report looks at AI national strategies progress and future steps," European Commission, June 22, 2021, https://digital-strategy.ec.europa.eu/en/news/new-report-looks-ai-national-strategies-progress-and-future-steps.
67. "White paper on artificial intelligence: a European approach to excellence and trust," European Commission, February 19, 2020, https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.
68. "Coordinated plan on artificial intelligence 2021 review," European Commission, April 21, 2021, https://digital-strategy.ec.europa.eu/en/library/coordinated-plan-artificial-intelligence-2021-review.
69. "The AI Act (COM/2021/206 final)," European Commission, April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.
70. "New rules for artificial intelligence—questions and answers," European Commission, April 21, 2021, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683.
71. "New rules for artificial intelligence—questions and answers," European Commission, April 21, 2021, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_1683.
72. "The AI Act (COM/2021/206 final)," Title V, p. 69, European Commission, April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206; "Four ICT48 networks of AI excellence centres," VISION, accessed August 25, 2021, https://www.vision4ai.eu/vision4ai/community/.
73. "EU-funded projects that use artificial intelligence technology," European Commission, April 21, 2021, https://digital-strategy.ec.europa.eu/en/news/eu-funded-projects-use-artificial-intelligence-technology; "Digital Europe Programme: A proposed €7.5 billion of funding for 2021-2017," European Commission, December 14, 2020, https://digital-strategy.ec.europa.eu/en/library/digital-europe-programme-proposed-eu75-billion-funding-2021-2027.
74. "Communication from the Commission to the European Parliament, the Council, the European Economic and Social Commmittee, and the Committee of the Regions: A European strategy for data," European Commission, February 19, 2020, https://ec.europa.eu/info/sites/default/files/communication-european-strategy-data-19feb2020_en.pdf; "The Digital Services Act package," European Commission, updated April 26, 2021, https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package; "Cybersecurity policies," European Commission, updated July 1, 2021, https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-policies; "Europe's Digital Decade—questions and answers," European Commission, March 9, 2021, https://ec.europa.eu/commission/presscorner/detail/en/QANDA_21_984; "Public consultation on a set of European digital principles," European Commission, May 12, 2021, https://digital-strategy.ec.europa.eu/en/consultations/public-consultation-set-european-digital-principles.
75. "Special Committee on Artificial Intelligence in a Digital Age," European Parliament, accessed August 26, 2021, https://www.europarl.europa.eu/committees/en/aida/home/highlights; "STOA Centre for Artificial Intelligence (C4AI)," European Parliament, Panel for the Future of Science and Technology (STOA), accessed August 26, 2021, https://www.europarl.europa.eu/stoa/en/centre-for-AI.
76. "The AI Act (COM/2021/206 final)," p. 5, European Commission, April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.
77. "The AI Act (COM/2021/206 final)," p. 14, European Commission, April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.
78. "The European AI Alliance," European Commission, updated June 23, 2021, https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance; "EU-US launch Trade and Technology Council to lead values-based global digital transformation," European Commission, June 15, 2021, https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2990.
79. "Society 5.0," Cabinet Office, Government of Japan, accessed August 25, 2021, https://www8.cao.go.jp/cstp/english/society5_0/index.html.
80. "Social principles of human-centric AI (draft)," Cabinet Office, Government of Japan, https://www8.cao.go.jp/cstp/stmain/aisocialprinciples.pdf.
81. "The Prime Minister in action: Industrial Competitiveness Council," Prime Minister of Japan and His Cabinet, May 19, 2016, https://japan.kantei.go.jp/97_abe/actions/201605/19article8.html.
82. "AI governance in Japan Ver. 1.0: interim report," Ministry of Economy, Trade, and Industry, Expert Group on Architecture for AI Principles to be Practiced, January 15, 2021, https://www.meti.go.jp/press/2020/01/20210115003/20210115003-3.pdf.
83. "AI governance in Japan Ver. 1.0: interim report," Ministry of Economy, Trade, and Industry, Expert Group on Architecture for AI Principles to be Practiced, January 15, 2021, https://www.meti.go.jp/press/2020/01/20210115003/20210115003-3.pdf.
84. "Draft AI R&D guidelines for international discussions," The Conference toward AI Network Society, July 28, 2017, https://www.soumu.go.jp/main_content/000507517.pdf.
85. "Social principles of human-centric AI," Cabinet Office, Government of Japan, 2019, https://www.cas.go.jp/jp/seisaku/jinkouchinou/pdf/humancentricai.pdf.
86. "AI utilization guidelines: practical reference for AI utilization," The Conference toward AI network society," August 9, 2019, https://www.soumu.go.jp/main_content/000658284.pdf.
87. "AI utilization guidelines: practical reference for AI utilization," The Conference toward AI network society," August 9, 2019, https://www.soumu.go.jp/main_content/000658284.pdf.

88. "Global Technology Governance Summit," World Economic Forum, April 6–8, 2021, https://www.weforum.org/events/global-technology-governance-summit-2021.

89. "AI governance in Japan Ver. 1.0: interim report," Ministry of Economy, Trade, and Industry, Expert Group on Architecture for AI Principles to be Practiced, January 15, 2021, https://www.meti.go.jp/press/2020/01/20210115003/20210115003-3.pdf.

90. "Transforming Singapore through technology," Smart Nation Singapore, updated August 12, 2021, https://www.smartnation.gov.sg/why-Smart-Nation/transforming-singapore.

91. "National AI Strategy: the next key frontier of Singapore's Smart Nation Journey," Smart Nation Singapore, updated July 1, 2021, https://www.smartnation.gov.sg/why-Smart-Nation/NationalAIStrategy.

92. "National AI Strategy: the next key frontier of Singapore's Smart Nation Journey," Smart Nation Singapore, updated July 1, 2021, https://www.smartnation.gov.sg/why-Smart-Nation/NationalAIStrategy.

93. "AI Singapore," accessed August 25, 2021, https://aisingapore.org/; "AI Singapore," National Research Foundation, Prime Minister's Office Singapore, accessed August 25, 2021, https://www.nrf.gov.sg/programmes; Hodan Omaar, "U.S. states can succeed in AI by looking at Singapore," U.S. News & World Report, November 27, 2020, https://www.usnews.com/news/best-states/articles/2020-11-27/how-us-states-can-succeed-in-ai-by-looking-at-singapore.

94. "First comprehensive trusted data sharing framework now available," Personal Data Protection Commision Singapore, June 28, 2019, https://www.pdpc.gov.sg/news-and-events/announcements/2019/06/first-comprehensive-trusted-data-sharing-framework-now-available.

95. "First comprehensive trusted data sharing framework now available," Personal Data Protection Commision Singapore, June 28, 2019, https://www.pdpc.gov.sg/news-and-events/announcements/2019/06/first-comprehensive-trusted-data-sharing-framework-now-available.

96. "Model artificial intelligence governance framework: second edition," Personal Data Protection Commission Singapore, January 2020, https://www.pdpc.gov.sg/help-and-resources/2020/01/second-edition-of-model-artificial-intelligence-governance-framework.

97. "AI sector deal," UK Department for Business, Energy, & Industrial Strategy and Department for Digital, Culture, Media, & Sport, updated May 21, 2019, https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal.

98. "AI roadmap," UK Office for Artificial Intelligence, Department for Business, Energy, & Industrial Strategy, and Department for Digital, Culture, Media, & Sport, January 6, 2021, https://www.gov.uk/government/publications/ai-roadmap.

99. "A guide to using artificial intelligence in the public sector," Government Digital Service, Office for Artificial Intelligence, January 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/964787/A_guide_to_using_AI_in_the_public_sector__Mobile_version_.pdf.

100. "Department of Culture, Media & Sport, "Data: A new direction, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file1016395/Data_Reform_Consultation_Document__Accessible_.pdf.

101. "AI roadmap," p. 25, UK Office for Artificial Intelligence, Department for Business, Energy, & Industrial Strategy, and Department for Digital, Culture, Media, & Sport, January 6, 2021, https://www.gov.uk/government/publications/ai-roadmap.

102. "Carbis Bay G7 Summit Communique", G-7, June 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1001128/Carbis_Bay_G7_Summit_Communique__PDF__430KB__25_pages_.pdf.

103. "Preparing for the future of artificial intelligence," Executive Office of the President, National Science and Technology Council, Committee on Technology, October 2016, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf.

104. "The national artificial intelligence research and strategic development plan," Executive Office of the President, National Science and Technology Council, Networking and Information Technology Research and Development Subcommittee, October 2016, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/national_ai_rd_strategic_plan.pdf.

105. "The national artificial intelligence research and development strategic plan: 2019 update," National Science & Technology Council, Select Committee on Artificial Intelligence, June 2019, https://www.nitrd.gov/pubs/National-AI-RD-Strategy-2019.pdf.

106. "American artificial intelligence initiative: Year one annual report," The White House, Office of Science and Technology Policy, February 2020, https://www.nitrd.gov/nitrdgroups/images/c/c1/American-AI-Initiative-One-Year-Annual-Report.pdf.

107. William M. (Mac) Thornberry National Defense Authorization Act for Fiscal Year 2021, 15 U.S.C. § 9411, https://uscode.house.gov/view.xhtml;jsessionid=8825DF991DABFDFFEEA1C5B8D89DC5F0?req=10+USC&f=treesort&fq=true&num=7545&hl=true&edition=prelim&granuleId=USC-prelim-title12-section4640.

108. "Executive order 13960: Promoting the use of trustworthy artificial intelligence in the federal government," Executive Office of the President, December 3, 2020, https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government.

109. Russell T. Vought, "Memorand

um for the heads of executive departments and agencies," Executive Office of the President, Office of Management and Budget, November 17, 2020, https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf.

110. "Readout of the first National Artificial Intelligence Research Resource Task Force meeting," July 29, 2021, White House, https://www.whitehouse.gov/ostp/news-updates/2021/07/29/readout-of-the-first-national-artificial-intelligence-research-resource-task-force-meeting/.

111. Russell T. Vought, "Memorandum for the heads of executive departments and agencies," Executive Office of the President, Office of

Management and Budget, November 17, 2020, https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf.

112. "Global emerging technology summit: advancing prosperity, security, and innovation," The National Security Commission on Artificial Intelligence, July 13, 2021, https://www.nscai.gov/all-events/summit/.
113. "G7 ICT and Industry Ministers' Declaration: Making the next production revolution inclusive, open, and secure," G-7, September 27, 2017, http://www.g8.utoronto.ca/ict/2017-ict-declaration.html.
114. "Charlevoix common vision for the future of artificial intelligence," G-7, 2018, https://www.mofa.go.jp/files/000373837.pdf.
115. "G7 Multistakeholder Conference on Artificial Intelligence: Final Summary Report," Government of Canada, accessed September 21, 2021, https://www.ic.gc.ca/eic/site/133.nsf/eng/00007.html.
116. "Setting principles for the digital economy: Establishing a G7 data and technology forum," Mastercard, March 22, 2021, https://www.mastercard.com/news/research-reports/2021/setting-principles-for-the-digital-economy-establishing-a-g7-data-and-technology-forum/.
117. "G7 tech leaders agree bold new proposals to boost online safety worldwide," G-7, April 28, 2021, https://www.g7uk.org/g7-tech-leaders-agree-bold-new-proposals-to-boost-online-safety-worldwide/.
118. "France and Canada create new expert international panel on artificial intelligence," Government of France, December 7, 2018, https://www.gouvernement.fr/en/france-and-canada-create-new-expert-international-panel-on-artificial-intelligence.
119. The Global Partnership on Artificial Intelligence, accessed August 25, 2021, https://www.gpai.ai/about/.
120. "The special G20 event on artificial intelligence and robotics," G-20 Italia 2021, July 19, 2021, https://www.g20.org/the-special-g20-event-on-artificial-intelligence-and-robotics.html.
121. "D5 London: about D5 member countries," UK Cabinet Office and Government Digital Service," December 9, 2014, https://www.gov.uk/government/news/d5-london-about-d5-member-countries.
122. Joshua P. Meltzer and Cameron F. Kerry, "Strengthening international cooperation on artificial intelligence," The Brookings Institution, February 17, 2021, https://www.brookings.edu/research/strengthening-international-cooperation-on-artificial-intelligence/.
123. OECD, "The State of Implementation of the OECD AI Principles," (June 18, 2021), https://www.oecd.org/digital/state-of-implementation-of-the-oecd-ai-principles-1cd40c44-en.htm
124. http://globalpolicy.ai.
125. "AI forums guide," Global Partners Digital, accessed August 25, 2021, https://www.gp-digital.org/case-study/ai-forums-guide/.
126. "Elaboration of a recommendation on the ethics of artificial intelligence," UNESCO, accessed September 1, 2021, https://en.unesco.org/artificial-intelligence/ethics; "First draft of the recommendation on the ethics of artificial intelligence," United Nations Educational, Scientific, and Cultural Organization, UNESDOC Digital Library,, September 7, 2020, https://unesdoc.unesco.org/ark:/48223/pf0000373434.;"Implementing the Secretary-General's roadmap for digital cooperation," United Nations Office of the Secretary-General's Envoy on Technology, April 2021, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/Update_on_Roadmap_implementation_April_2021.pdf.
127. "Implementing the Secretary-General's roadmap for digital cooperation," United Nations Office of the Secretary-General's Envoy on Technology, April 2021, https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/Update_on_Roadmap_implementation_April_2021.pdf.
128. "CAHAI—Ad hoc Committee on Artificial Intelligence," Council of Europe Portal, accessed September 1, 2021, https://www.coe.int/en/web/artificial-intelligence/cahai.
129. "Ad hoc committee on artificial intelligence (CAHAI): Feasibility study," Council of Europe, December 17, 2020, https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da.
130. "Ad hoc committee on artificial intelligence (CAHAI): Feasibility study," Council of Europe, December 17, 2020, https://rm.coe.int/cahai-2020-23-final-eng-feasibility-study-/1680a0c6da.
131. "Global AI Action Alliance," World Economic Forum, accessed August 25, 2021, https://www.weforum.org/projects/global-ai-action-alliance.
132. "Global AI Action Alliance," World Economic Forum, accessed August 25, 2021, https://www.weforum.org/projects/global-ai-action-alliance.
133. "EU and Japan step up cooperation in science, technology, and innovation," European Commission, May 26, 2020, https://ec.europa.eu/info/news/eu-and-japan-step-cooperation-science-technology-and-innovation-2020-may-26_en; "Artificial intelligence: Canada and France work with international community to support the responsible use of AI," Government of France, May 17, 2019, https://www.gouvernement.fr/en/artificial-intelligence-canada-and-france-work-with-international-community-to-support-the; "Memorandum of understanding between the Government of the Republic of Singapore and the Government of Australia on cooperation on artificial intelligence," March 23, 2020, https://www.mti.gov.sg/-/media/MTI/Microsites/DEAs/Singapore-Australia-Digital-Economy-Agreement/MOUs/MOU-on-Cooperation-on-Artificial-Intelligence.pdf; Dipanjan Roy Chaudhury, "India, Germany to explore partnership in AI during Merkel-Modi meet," The Economic Times, October 25, 2019, https://economictimes.indiatimes.com/news/politics-and-nation/india-germany-to-explore-partnership-in-ai-during-merkel-modi-meet/articleshow/71760304.cms.
134. "D5 London: about D5 member countries," UK Cabinet Office and Government Digital Service," December 9, 2014, https://www.gov.uk/government/news/d5-london-about-d5-member-countries.
135. "AI Partnership for Defense is a Step in the Right Direction – But Will Face Challenges", Lena Trabucco, October 5, 2020, http://opiniojuris.org/2020/10/05/ai-partnership-for-defense-is-a-step-in-the-right-direction-but-will-face-challenges/.

136. "Federal participation in the development and use of voluntary consensus standards and in conformity assessment activities," U.S. Office of Management and Budget, February 10, 1998, https://www.whitehouse.gov/wp-content/uploads/2017/11/Circular-119-1.pdf; "Regulation No. 1025/2021 on European standardisation," European Commission, October 25, 2012, https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:316:0012:0033:EN:PDF.

137. "Carbis Bay G7 summit communique," The White House, June 13, 2021, https://www.whitehouse.gov/briefing-room/statements-releases/2021/06/13/carbis-bay-g7-summit-communique/.

138. "G20: Call to action on international standards," MyITU, April 11, 2020, https://www.itu.int/en/myitu/News/2020/11/04/17/32/G20-call-to-action-on-international-standards.

139. "International co-operation for trustworthy AI (Principle 2.5)," OECD.AI Policy Observatory, accessed September 1, 2021, https://oecd.ai/dashboards/ai-principles/P14.

140. "Principles for the Development of International Standards, Guides and Recommendations," World Trade Organization, 2000, https://www.wto.org/english/tratop_e/tbt_e/principles_standards_tbt_e.htm.

141. Jonathan E. Hillman, "A´China Model?` Beijing´s Promotion of Alternative Global Norms and Standards," Testimony Before the U.S.-China Economic and Security Review Commission, Mar 13, 2020, https://www.csis.org/analysis/china-model-beijings-promotion-alternative-global-norms-and-standards.

142. "IEEE P7000—Engineering methodologies for ethical life-cycle concerns working group," IEEE Standards Association, accessed September 1, 2021, https://sagroups.ieee.org/7000/.

143. Tim Buthe and Walter Mattli, The New Global Rulers: The Privatization of Regulation in the World Economy (Princeton University Press, 2011), p. 30.

144. "Shaping the future of technology governance: Artificial intelligence and machine learning," World Economic Forum, accessed September 1, 2021, https://www.weforum.org/platforms/shaping-the-future-of-technology-governance-artificial-intelligence-and-machine-learning.

145. "Ethics guidelines for trustworthy AI," European Commission, updated March 8, 2021, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.

146. "High-level expert group on artificial intelligence," European Commission, June 23, 2021, https://ec.europa.eu/digital-single-market/en/high-level-expert-group-artificial-intelligence.

147. "Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment," European Commission, updated March 8, 2021, https://ec.europa.eu/digital-single-market/en/news/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment.

148. "The European AI Alliance," European Commission, updated June 23, 2021, https://digital-strategy.ec.europa.eu/en/policies/european-ai-alliance.

149. "Our alliance is accelerating responsible artificial intelligence," World Economic Forum, accessed September 20, 2021, https://www.weforum.org/our-impact/a-new-alliance-is-ensuring-responsible-global-ai/.

150. See www.ethicssstandards.org.

151. "Publications," AI Now Institute, accessed September 1, 2021, https://ainowinstitute.org/reports.html.

152. Also see, for broader comparisons: Thilo Hagendorff, "The ethics of AI ethics: An evaluation of guidelines," Minds and Machines, February 1, 2020, https://doi.org/10.1007/s11023-020-09517-8.

153. "Comparing international frameworks for the development of responsible AI," BSA | The Software Alliance, accessed August 27, 2021, https://ai.bsa.org/global-ai-principles-framework-comparison/.

154. In past debates, such as the open public consultation carried out by the European Commission on its white paper in 2020, views have varied significantly. Industry typically is willing to narrow down the definition of machine learning and reluctant to cover commonly-used software under the definition of AI. On the other hand, civil society organization and digital rights activists propose the extension of the definition to any and all forms of automated decision making. See Andrea Renda et al., "Study to support an impact assessment of regulatory requirements for the artificial intelligence in Europe," European Commission, April 2021, https://op.europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1.

155. "Artificial intelligence in society," OECD iLibrary, accessed September 1, 2021, https://www.oecd-ilibrary.org/sites/8b303b6f-en/index.html?itemId=/content/component/8b303b6f-en.

156. Stefan Hajkowicz, et al., "Artificial intelligence: Solving problems, growing the economy, and improving our quality of life," Commonwealth Scientific and Industrial Research Organisation (CSIRO), November 14, 2019, https://apo.org.au/node/268341.

157. "Australia's AI action plan," Australian Government, June 2021, https://www.industry.gov.au/sites/default/files/June%202021/document/australias-ai-action-plan.pdf.

158. In the Japanese guidelines, a classification is provided encompassing '(i) general-purpose AI, based on the concept of creating machines that possess human intelligence itself ("Strong AI"), and (ii) AI based on the concept of causing machines to perform activities that humans use their intelligence to perform ("Weak AI"), whereas the Guidelines refer to "Weak AI" only.

159. "Contract guidelines on utilization of AI and data," Ministry of Economy, Trade, and Industry, June 2018, https://www.meti.go.jp/press/2019/04/20190404001/20190404001-2.pdf.

160. "Model artificial intelligence governance framework: second edition," Personal Data Protection Commission Singapore, January 2020,

https://www.pdpc.gov.sg/-/media/files/pdpc/pdf-files/resource-for-organisation/ai/sgmodelaigovframework2.pdf.

161. "A guide to using artificial intelligence in the public sector," Central Digital and Data Office, Office for Artificial Intelligence, The Rt Hon. Oliver Dowden CBE MP, Margot James, and The Rt Hon. Chris Skidmore MP, June 10, 2019, https://www.gov.uk/government/publications/understanding-artificial-intelligence.

162. Karine Perset, et al., "A first look at the OECD's framework for the classification of AI systems, designed to give policymakers clarity," OECD Policy Observatory, November 24, 2020, https://www.oecd.ai/wonk/a-first-look-at-the-oecds-framework-for-the-classification-of-ai-systems-for-policymakers.

163. See: "Digital Economy," U.S.-Japan Business Council and the Japan-U.S. Business Council, 2019, https://www.uschamber.com/file/25475/download: "Any efforts by the two governments in this area should be mindful of existing rules and regulations, incorporate risk-based approaches to AI governance … ."

164. Russell T. Vought, "Memorandum for the heads of executive departments and agencies," Executive Office of the President, Office of Management and Budget, November 17, 2020, https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf.

165. "Request for information for development of Artificial Intelligence Risk Management Framework," National Institute of Standards and Technology, July 29, 2021, https://www.federalregister.gov/documents/2021/07/29/2021-16176/artificial-intelligence-risk-management-framework.

166. Andrea Renda et al., "Study to support an impact assessment of regulatory requirements for the artificial intelligence in Europe," European Commission, April 2021, https://op.europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1.

167. Charles Bradley, Richard Wingfield, and Megan Metzger, "National artificial intelligence strategies and human rights: A review," Global Partners Digital and Global Digital Policy Incubator at the Stanford Cyber Policy Center, April 2020, https://www.gp-digital.org/wp-content/uploads/2020/04/National-Artifical-Intelligence-Strategies-and-Human-Rights%E2%80%94A-Review_.pdf.

168. "Opinion of the Data Ethics Commission," German Data Ethics Commission (GDEC), 2020,https://www.bmjv.de/SharedDocs/Downloads/DE/Themen/Fokusthemen/Gutachten_DEK_EN_lang.pdf?__blob=publicationFile&v=3.

169. See e.g., Sarah Kamensky, "Artificial intelligence and technology in health care: Overview and possible legal implications," DePaul Journal of Health Care Law, 2020, https://via.library.depaul.edu/cgi/viewcontent.cgi?article=1382&context=jhcl; also see Urs J. Muehlematter, Paola Daniore, and Kerstin N. Vokinger, "Approval of artificial intelligence and machine learning-based medical devices in the USA and Europe (2015-20): A comparative analysis," Lancet Digit Health ,January 18, 2021, https://www.thelancet.com/action/showPdf?pii=S2589-7500%2820%2930292-2.

170. "NIST requests information to help develop an AI risk management framework," National Institute of Standards and Technology, July 29, 2021, https://www.nist.gov/news-events/news/2021/07/nist-requests-information-help-develop-ai-risk-management-framework.

171. This context is dedicated to regulatory cooperation and does not deal with important debates related to military uses of AI, such as the case of lethal autonomous weapons.

172. For example, the ongoing consultation on a risk management guidance for AI at the U.S. National Institute of Standards and Technology (NIST) will cover aspects that are similar to those discussed in many other legal systems, including the European Union. See "NIST requests information to help develop an AI risk management framework," National Institute of Standards and Technology, July 29, 2021, https://www.nist.gov/news-events/news/2021/07/nist-requests-information-help-develop-ai-risk-management-framework.

173. For a repository, see: "AI frameworks, guidelines, toolkits," AI Ethicist, accessed August 27, 2021, https://www.aiethicist.org/frameworks-guidelines-toolkits.

174. Jonathan B. Wiener, et al., The reality of precaution: Comparing risk regulation in the United States and Europe (Routledge, 2010).

175. The U.S. assesses AI risks along three broad criteria: 1. Overall assessment of type of risks that are acceptable vs. type of risks that present possibility of unacceptable harm; 2. risk assessment should be informed by magnitude and nature of consequences should an AI tool fail (or succeed); 3. where practical and consistent with law, risk assessment/management shall be applied to similar AI functionalities and across sectors. See: Russell T. Vought, "Memorandum for the heads of executive departments and agencies," Executive Office of the President, Office of Management and Budget, November 17, 2020, https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf.

176. Under the EU' AI regulation, assessment through internal control checks for high-risk AI systems outside existing regulatory regimes would require a full, effective, and documented ex ante compliance with all requirements of the regulation and with robust quality and risk management systems and monitoring after deployment.

177. Mona Sloane and Andrea Renda, "Now is the time for a transatlantic dialog on the risk of AI," VentureBeat, April 23, 2021, https://venturebeat.com/2021/04/23/now-is-the-time-for-a-transatlantic-dialog-on-the-risk-of-ai/.

178. "Artificial intelligence: An accountability framework for federal agencies and other entities," Government Accountability Office, June 2021, https://www.gao.gov/assets/720/716110.pdf.

179. "Singapore's approach to AI governance," Personal Data Protection Commission Singapore, accessed September 1, 2021, https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework.

180. "The Japanese Society for Artificial Intelligence ethical guidelines," Japanese Society for Artificial Intelligence, May 2017, http://ai-elsi.org/archives/514.

181. "The assessment list for trustworthy artificial intelligence," European Commission's High-Level Expert Group on Artificial Intelligence, accessed September 1, 2021, https://altai.insight-centre.org/.

182. "Ethically aligned design: A vision for prioritizing human well-being with autonomous and intelligent systems," IEEE, 2019, https://ethicsinaction.ieee.org/.

183. Christian Berghoff, et al., "Towards auditable AI systems: Current status and future directions," TUV Verband, Federal Office for Information Security, and Fraunhofer HHI, May 2021, https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/KI/Towards_Auditable_AI_Systems.pdf?__blob=publicationFile&v=4.

184. "AI auditing framework," UK Information Commissioner's Office, accessed September 1, 2021, https://ico.org.uk/about-the-ico/news-and-events/ai-auditing-framework/.

185. Inioluwa Debora Raji, et al., "Closing the AI accountability gap: Defining an end-to-end framework for internal algorithmic auditing," Conference on Fairness, Accountability, and Transparency (FAT* '20), January 27-30, 2020, https://arxiv.org/pdf/2001.00973.pdf.

186. "Ethics and governance of artificial intelligence for health," World Health Organization, June 28, 2021, https://www.who.int/publications/i/item/9789240029200.

187. The first round of analysis was based on the attributes in the catalogue and focused on the top 64 shortlisted initiatives. See: "Areas for future action in the responsible AI ecosystem," The Future Society, December 2020, https://gpai.ai/projects/responsible-ai/areas-for-future-action-in-responsible-ai.pdf.

188. Among the existing initiatives in countries that participate in the FCAI, it is worth highlighting the UK Information Commissioner Office's Guidance on AI Auditing Framework, which covers best practices in the development and deployment of AI systems for ensuring compliance with data protection laws. The Guidance offers organizations a self-regulatory framework for assessing data protection risks associated with the use of AI systems and makes recommendations on the best technical and organizational measures for mitigating those risks. The key themes of the Guidance are accountability and governance; data protection; lawfulness, fairness, and transparency; security and data minimisation; and ensuring that individuals can effectively exercise their rights relating to their data. See: "AI auditing framework," UK Information Commissioner's Office, accessed August 27, 2021, https://ico.org.uk/about-the-ico/news-and-events/ai-auditing-framework/.

189. "Policy on the compliance assistance sandbox," U.S. Bureau of Consumer Financial Protection, September 10, 2019, https://files.consumerfinance.gov/f/documents/cfpb_final-policy-on-cas.pdf.

190. "Regulatory sandbox," UK Information Commissioner's Office, accessed September 1, 2021, https://www.oecd.ai/dashboards/policy-initiatives/2019-data-policyInitiatives-24319; "Sandbox for responsible artificial intelligence," Norway Datatilsynet, accessed September 1, 2021, https://www.datatilsynet.no/en/regulations-and-tools/sandbox-for-artificial-intelligence/; "A GDPR 'sandbox' to support innovative projects in the field of digital health," CNIL, February 15, 2021, https://www.cnil.fr/fr/un-bac-sable-rgpd-pour-accompagner-des-projets-innovants-dans-le-domaine-de-la-sante-numerique.

191. OECD.ai Policy Observatory, accessed September 1, 2021, https://www.oecd.ai/dashboards/policy-initiatives/2019-data-policyInitiatives-24294.

192. "The AI Act (COM/2021/206 final)," Articles 44 and 45, European Commission, April 21, 2021, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence.

193. "The Centers of Excellence," U.S. General Services Administration, accessed September 1, 2021, https://www.gsa.gov/about-us/organization/federal-acquisition-service/technology-transformation-services/the-centers-of-excellence.

194. "AI procurement in a box," World Economic Forum, June 11, 2020, https://www.weforum.org/reports/ai-procurement-in-a-box.

195. Mona Sloane, et al., "AI and procurement—a primer," New York University, June 28, 2021, https://archive.nyu.edu/handle/2451/62255.

196. For a description of specific issues raised by AI in seven sectors, see: Christoph Lütge, et al., "AI4 People's 7 AI Global Frameworks," https://ai4people.eu/wp-content/pdf/AI4People7AIGlobalFrameworks.pdf.

197. "Request for information and comment on financial institutions' use of artificial intelligence, including machine learning, Federal Register, Vol. 86, No. 60, March 31, 2021, https://www.govinfo.gov/content/pkg/FR-2021-03-31/pdf/2021-06607.pdf?utm_campaign=subscription+mailing+list&utm_source=federalregister.gov&utm_medium=email.

198. "Artificial intelligence/machine learning (AI/ML)-based software as a medical device (SaMD) action plan," U.S. Food & Drug Administration, January 2021, https://www.fda.gov/medical-devices/software-medical-device-samd/artificial-intelligence-and-machine-learning-software-medical-device.

199. Nao Aisu, Masahiro Miyake, Kohei Takeshita, Masato Akiyama, Ryo Kawasaki, Kenji Kashiwagi, Taiji Sakamoto, Tetsuro Oshika, Akitaka Tsujikawa, "Regulatory-approved Deep Learning/Machine Learning-Based Medical Devices in Japan as of 2020: A Systematic Review," medRxiv 2021.02.19.21252031; https://www.medrxiv.org/content/10.1101/2021.02.19.21252031v1.article-info.

200. "A European strategy for data," European Commission, updated August 11, 2021, https://digital-strategy.ec.europa.eu/en/policies/strategy-data.

201. Denis McCauley, "The global AI agenda," MIT Technology Review Insights, 2020, https://mittrinsights.s3.amazonaws.com/AIagenda2020/GlobalAIagenda.pdf.

202. "Working group on data governance," The Global Partnership on Artificial Intelligence (GPAI), accessed June 1, 2021, https://gpai.ai/projects/data-governance/.

203. "Artificial intelligence: A worldwide overview of AI patents and patenting by the UK AI sector," UK Intellectual Property Office, June 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/817610/Artificial_Intelligence_-_A_worldwide_overview_of_AI_patents.pdf; "New benchmark USPTO study finds artificial intelligence in U.S. patents rose by more than

100% since 2002," U.S. Patent and Trademark Office, October 27, 2020, https://www.uspto.gov/about-us/news-updates/new-benchmark-uspto-study-finds-artificial-intelligence-us-patents-rose-more; Gregory Discher, "AI update: USPTO releases report on growth of artificial intelligence applications," Inside Tech Media, https://www.lexology.com/library/detail.aspx?g=d183b303-5943-45ce-a639-15852900e8a4.

204. Sven Herpig, "Securing artificial intelligence," Stiftung Neue Verantwortung, October 17, 2019, https://www.stiftung-nv.de/de/publikation/securing-artificial-intelligence.

205. Broadly speaking, there are three models for privacy that are evolving: the U.S., the EU and the Chinese model. The divergence between the U.S. and EU approaches to privacy, especially given the breakdown of transatlantic data flows of personal data following the Schrems II decision by the CJEU, is potentially a significant barrier to cooperation on AI. China's Personal Information Protection Law is loosely modeled on GDPR, with enhanced obligations for platforms and restrictions on cross-border data flows; in addition, in June 2021, China passed its Data Security Law that includes comprehensive obligations on domestic processing and storage of data, including a category of "important data," as yet to be defined, that will likely also apply to personal data. See: Cameron F. Kerry, "The oracle at Luxembourg: The EU Court of Justice judges the world on surveillance and privacy," The Brookings Institution, January 11, 2021, https://www.brookings.edu/research/the-oracle-at-luxembourg-the-eu-court-of-justice-judges-the-world-on-surveillance-and-privacy/.

206. As an early adopter of data protection laws and a judge of other countries' privacy and data protection regimes, the European Union has wide influence over privacy laws around the world. According to Graham Greenleaf, some 141 countries have adopted national laws on privacy by 2018; a substantial majority of these resemble the GDPR with rights for individuals ("data subjects") with obligations on the entities that process personal data ("controllers" or "processors") based on established fair information practice principles that include lawful grounds for processing and data minimization. See: Graham Greenleaf, "Global tables of data privacy laws and bills," Supplement to 157 Privacy Laws & Business International Report, May 30, 2019, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3380794.

207. Cameron F. Kerry, "The oracle at Luxembourg: The EU Court of Justice judges the world on surveillance and privacy," The Brookings Institution, January 11, 2021, https://www.brookings.edu/research/the-oracle-at-luxembourg-the-eu-court-of-justice-judges-the-world-on-surveillance-and-privacy/.

208. APEC Cross-Border Privacy Rules (CBPR) System, accessed August 27, 2021, http://cbprs.org/.

209. "APEC endorses the first U.S. non-profit accountability agent," The National Law Review, January 26, 2001, https://www.natlawreview.com/article/apec-endorses-first-us-non-profit-accountability-agent#:~:text=To%20date%2C%20nine%20APEC%20economies,have%20endorsed%20the%20CBPR%20system.

210. Masumi Koizumi, "Japan's pitch for free data flows 'with trust' faces uphill battle at G20 amid 'splinternet' fears, The Japan Times, June 27, 2019, https://www.japantimes.co.jp/news/2019/06/27/business/tech/japans-pitch-free-data-flows-trust-faces-uphill-battle-g20-amid-splinternet-fears/.

211. Matthew P. Goodman and Pearl Risberg, "Advancing data governance in the G7," Center for Strategic & International Studies, February 2, 2021, https://www.csis.org/analysis/advancing-data-governance-g7.

212. Richard Samans and Sean Doherty, "Data Free Flow with Trust (DFFT): Paths towards free and trusted data flows," World Economic Forum, May 2020, http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf.

213. The CJEU upheld the validity of model contract clauses but ruled that companies and data protection regulatory bodies must make case-by-case decisions on whether a transfer may be subject to government access in a country outside the EU and, if so, either put in place "additional safeguards" against such access, or cease the transfers. The Privacy Shield prong of the decision affected some 5,300 U.S. and EU companies; the model clauses prong many more, throwing into doubt the status of transfers to many countries. See: "Privacy Shield List," International Trade Administration, accessed June 1, 2021, https://www.privacyshield.gov/list.

214. "Data protection—standard contractual clauses for transferring personal data to non-EU countries (implementing act)," European Commission draft implementing decision, November 12, 2020, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Commission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries_en; "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data," European Data Protection Board, November 10, 2020, https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

215. In October 2020, the French Conseil d'État approved the use of Microsoft Azure as a platform for French health data against the advice of the French data protection regulator, but only on the condition that the data would be stored in Europe and eventually shifted to a French or European provider; decisions or pending cases in Bavaria, Portugal, and Ireland follow similar lines. "France: Conseil d'Etat decision on Health Data Hub," OneTrust DataGuidance, October 2020, https://www.dataguidance.com/opinion/france-conseil-detat-decision-health-data-hub.

216. Anupam Chander, "Is data localization a solution for Schrems II?" Journal of International Economic Law, September 2020, https://academic.oup.com/jiel/article-abstract/23/3/771/5909035?redirectedFrom=fulltext.

217. "Government access to personal data held by the private sector: Statement by the OECD Committee on Digital Economy Policy," OECD, December 22, 2020, https://www.oecd.org/digital/trusted-government-access-personal-data-private-sector.htm.

218. Josh Horwitz, "China passes new personal data privacy law, to take effect Nov. 1," Reuters, August 20, 2021, https://www.reuters.com/world/china/china-passes-new-personal-data-privacy-law-take-effect-nov-1-2021-08-20/; "Questions and answers: Mandate for the Second Additional Protocol to the Budapest Convention," European Commission, February 5, 2019, https://ec.europa.eu/commission/presscorner/detail/cs/MEMO_19_865.

219. Anirudh Burman and Upasana Sharma, "How would data localization benefit India?" Carnegie India, April 14, 2021, https://carnegieindia.org/2021/04/14/how-would-data-localization-benefit-india-pub-84291.

220. See: Samuel Warren and Louis Brandeis, "The right to privacy," Harvard Law Review Vol. IV No. 5, December 15, 1890, https://groups.csail.mit.edu/mac/classes/6.805/articles/ privacy/Privacy_brand_warr2.html.

221. Ian Brown et al., "Towards multilateral standards for surveillance reform," in Russell A. Miller, Privacy and Power: A Transatlantic Dialogue in the Shadow of the NSA-Affair (Cambridge: Cambridge University Press, 2017), pp.461–491, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2551164.

222. "General Data Protection Regulation, Article 89," European Commission, April 27, 2016, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679.

223. "Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data," European Data Protection Board, November 10, 2020, https://edpb.europa.eu/sites/default/files/consultation/edpb_recommendations_202001_supplementarymeasurestransferstools_en.pdf.

224. "International sharing of personal health data for research," European Academies Science Advisory Council, April 2021, https://easac.eu/publications/details/international-sharing-of-personal-health-data-for-research/.

225. "Open science for the 21st century: draft ISC working paper," International Science Council, June 2020, https://council.science/wp-content/uploads/2020/06/International-Science-Council_Open-Science-for-the-21st-Century_Working-Paper-2020_compressed.pdf.

226. "Multi-stakeholder forum on open government," Government of Canada, updated July 27, 2021, https://open.canada.ca/en/multi-stakeholder-forum-open-government.

227. "Canada's 2018–2020 National Action Plan on Open Government," Government of Canada, updated October 9, 2020, https://open.canada.ca/en/content/canadas-2018-2020-national-action-plan-open-government.

228. EU Open Data Portal, accessed August 27, 2021, https://data.europa.eu/en.

229. "A European strategy for data," European Commission, updated June 25, 2021, https://ec.europa.eu/digital-single-market/en/european-strategy-data.

230. "Data Governance Act (COM/2020/767 final),", European Commission, November 25, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767.

231. "Japan open data charter action plan," October 29, 2013, http://japan.kantei.go.jp/policy/it/2013/1029_fulltext.pdf.

232. "Factsheet: data.gov.sg," GovTech Singapore, https://www.tech.gov.sg/files/products-and-services/9-Datagovsg-Factsheet.pdf; "Developer guide," Government of Singapore, accessed August 27, 2021, https://data.gov.sg/developer.

233. "Open data white paper: Unleashing the potential," UK Minister of State for the Cabinet Office and Paymaster General by Command of Her Majesty, June 2012, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/78946/CM8353_acc.pdf.

234. "Government transformation strategy: better use of data," Government Digital Service, Cabinet Office, February 9, 2017, https://www.gov.uk/government/publications/government-transformation-strategy-2017-to-2020/government-transformation-strategy-better-use-of-data.

235. "AI sector deal," UK Department for Business, Energy, & Industrial Strategy and Department for Digital, Culture, Media, & Sport, updated May 21, 2019, https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal.

236. "National data strategy," Department for Digital, Culture, Media, & Sport, December 9, 2020, https://www.gov.uk/government/publications/uk-national-data-strategy/national-data-strategy.

237. OPEN Government Data Act, H.R. 1770, 115th Cong. (2017), https://www.congress.gov/bill/115th-congress/house-bill/1770; "About data.gov," data.gov, accessed September 9, 2021, https://www.data.gov/about#who.

238. "About us," GISAID, accessed August 27, 2021, https://www.gisaid.org/about-us/mission/; "GenBank Overview," National Center for Biotechnology Information, accessed August 27, 2021, https://www.ncbi.nlm.nih.gov/genbank/; Stephanie Chin and Caitlin Chin, "To mitigate the costs of future pandemics, establish a common data space," The Brookings Institution, TechTank, November 2, 2020, https://www.brookings.edu/blog/techtank/2020/11/02/to-mitigate-the-costs-of-future-pandemics-establish-a-common-data-space/.

239. Julie Baloup, " The Data Governance Act: New rules for international transfers of non-personal data held by the public sector," https://europeanlawblog.eu/2021/06/10/the-data-governance-act-new-rules-for-international-transfers-of-non-personal-data-held-by-the-public-sector/.

240. "GTFS background," GTFS, accessed September 8, 2021, https://gtfs.org/gtfs-background.

241. "Feeds," OpenMobilityData, accessed September 8, 2021, https://transitfeeds.com/feeds.

242. "Introduction to the General Transit Feed Specification (GTFS) and Informal Transit System Mapping (Self-Paced)" The World Bank, accessed September 8, 2021, https://olcsb.worldbank.org/content/introduction-general-transit-feed-specification-gtfs-and-informal-transit-system-mapping.

243. "Evaluation of emerging air sensor performance," U.S. Environmental Protection Agency, September 8, 2021, https://www.epa.gov/air-sensor-toolbox/evaluation-emerging-air-sensor-performance.

244. Yang Wang, "Laboratory evaluation and calibration of three low-cost particle sensors for particulate matter measurement," September 7, 2015, https://www.tandfonline.com/doi/full/10.1080/02786826.2015.1100710.

245. Karoline K. Johnson, et al., "Field test of several low-cost particulate matter sensors in high and low concentration urban environments,"

Aerosol and Air Quality Research, January 30, 2018, https://aaqr.org/articles/aaqr-17-10-oa-0418.pdf.

246. Naomi Zimmerman, et al., "A machine learning calibration model using random forests to improve sensor performance for lower-cost air quality monitoring," Atmospheric Measurement Techniques, January 15, 2018, https://amt.copernicus.org/articles/11/291/2018/.

247. Hone-Jay Chu, Muhammad Zeeshan Ali, and Yu-Chen He, "Spatial calibration and PM2.5 mapping of low-cost air quality sensors," Scientific Reports, December 16, 2020, https://www.nature.com/articles/s41598-020-79064-w.

248. "Significant cyber incidents," Center for Strategic & International Studies, accessed August 27, 2021, https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

249. "Maximize collaboration through secure data sharing," Accenture, October 1, 2019, https://www.accenture.com/us-en/insights/digital/maximize-collaboration-secure-data-sharing.

250. Bharath K. Samanthula, "A secure data sharing and query processing framework via federation of cloud computing," Information Systems, Vol. 48, March 2015, https://www.sciencedirect.com/science/article/abs/pii/S0306437913001208.

251. Peichang Shi, et al., "Blockchain-based trusted data sharing among trusted stakeholders in IoT," August 1, 2019, https://onlinelibrary.wiley.com/doi/full/10.1002/spe.2739; Shangping Wang, Yinglong Zhang, and Yaling Zhang, "A blockchain-based framework for data sharing with fine-grained access control in decentralized storage systems," IEEE Access, June 29, 2018, https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=8400511.

252. "Maximize collaboration through secure data sharing," Accenture, October 1, 2019, https://www.accenture.com/us-en/insights/digital/maximize-collaboration-secure-data-sharing.

253. "About us," CSIRO, accessed August 27, 2021, https://data61.csiro.au/en/About; "The effective and ethical development of artificial intelligence: an opportunity to improve our wellbeing," Data 61 on behalf of the Australian Council of Learned Academies, 2018, https://acola.org/wp-content/uploads/2019/07/acola-ai-input-paper_data-integrity-standards-and-ethics_data61.pdf.

254. Alison Donnellan, "AFP using AI innovation to protect investigators from abhorrent material," CSIRO, July 30, 2019, https://algorithm.data61.csiro.au/afp-using-ai-innovation-to-protect-investigators-from-abhor.

255. "Fintel Alliance," Australian Government AUSTRAC, updated August 24, 2021, https://www.austrac.gov.au/about-us/fintel-alliance; John Edison, "Share information, be safe and fight financial crime: The rundown on homomorphic encryption," Oracle, Financial Services Blog, https://blogs.oracle.com/financialservices/post/share-information-be-safe-and-fight-financial-crime-the-rundown-on-homomorphic-encryption.

256. Basil Han, "Voices from the AISG federated learning lab," AI Singapore, October 23, 2020, https://aisingapore.org/2020/10/voices-from-the-aisg-federated-lab/; Basil Han, "Do great things together with federated learning," AI Singapore, January 29, 2021, https://aisingapore.org/2021/01/do-great-things-together-with-federated-learning/; Jianshu Weng, Maurice Manning, and Mark Choo, "A peek into Synergos—AI Singapore's federated learning system," AI Singapore, November 10, 2020, https://aisingapore.org/2020/11/a-peek-into-synergos-ai-singapores-federated-learning-system/.

257. "Singapore sets up new centers to research data privacy technologies," Techwire Asia, January 23, 2019, https://techwireasia.com/2019/01/singapore-sets-up-new-centers-to-research-data-privacy-technologies/; "Singapore to invest S$50 million over next five years to bolster digital trust capabilities," AP News, July 14, 2021, https://apnews.com/press-release/pr-newswire/technology-singapore-dc8803a1d899fb1c4b8b0138528963f9.

258. Edgar A. Whitley, "Trusted digital identity provision: gov.uk Verify's federated approach," Center for Global Development, November 2018, https://www.cgdev.org/publication/trusted-digital-identity-provision-gov-uk-verify-federated-approach.

259. John Edison, "Share information, be safe and fight financial crime: The rundown on homomorphic encryption," Oracle, Financial Services Blog, December 1, 2020, https://blogs.oracle.com/financialservices/post/share-information-be-safe-and-fight-financial-crime-the-rundown-on-homomorphic-encryption.

260. "A history of Census privacy protections," U.S. Census Bureau, October 10, 2019, https://www.census.gov/library/visualizations/2019/comm/history-privacy-protection.html; "Four ways new technology is revolutionizing the 2020 census," U.S. Census Bureau, May 19, 2020, https://www.census.gov/library/stories/2020/05/four-ways-new-technology-is-revolutionizing-the-2020-census.html.

261. "Final report," National Security Commission on Artificial Intelligence," March 2021, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

262. "Privacy enhancing technologies—a review of tools and techniques," Office of the Privacy Commissioner of Canada, Technology Analysis Division, November 2017, https://priv.gc.ca/en/opc-actions-and-decisions/research/explore-privacy-research/2017/pet_201711/.

263. "Privacy tech-know blog: Privacy enhancing technologies for businesses," Office of the Privacy Commissioner of Canada, April 12, 2021, https://priv.gc.ca/en/blog/20210412/.

264. "Hiroaki Kikuchi," Meiji University, accessed August 27, 2021, https://www.meiji.ac.jp/cip/english/frontline/kikuchi/index.html.

265. Hosuk Lee-Makiyama, et al., "Data Free Flow With Trust (DFFT): Paths toward free and trusted data flows," World Economic Forum, May 2020, http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf.

266. Jure Leskovec, "Web data: Amazon reviews," accessed August 27, 2021, https://snap.stanford.edu/data/web-Amazon.html.

267. ImageNet, updated March 11, 2021, https://image-net.org/.

268. Hannah Kuchler, "Pharma groups combine to promote drug discovery with AI," Financial Times, June 4, 2019, https://www.ft.com/content/

ef7be832-86d0-11e9-a028-86cea8523dc2.

269. Heiko Ludwig, Nathalie Baracaldo, and Gegi Thomas, "IBM federated learning—machine learning where the data is," IBM, August 21, 2020, https://www.ibm.com/blogs/research/2020/08/ibm-federated-learning-machine-learning-where-the-data-is/; Teresa Tung, et al., "Maximize collaboration through secure data sharing," Accenture, October 1, 2019, https://www.accenture.com/us-en/insights/digital/maximize-collaboration-secure-data-sharing.

270. "Data Governance Act (COM/2020/767 final),", European Commission, November 25, 2020, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020PC0767; Jetty Tielemans and Sam Jungyun Choi, "Proposal for an EU Data Governance Act—a first analysis," IAPP, December 10, 2020, https://iapp.org/news/a/proposal-for-an-eu-data-governance-act-a-first-analysis/.

271. "The AI Act (COM/2021/206 final)," Article 11, European Commission, April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.

272. "The AI Act (COM/2021/206 final)," Article 40, European Commission, April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206.

273. "Artificial intelligence measurement and evaluation at the National Institute of Standards and Technology," AIME Planning Team, June 14, 2021, https://www.nist.gov/system/files/documents/2021/06/16/AIME_at_NIST-DRAFT-20210614.pdf.

274. Peter Cihon, "Standards for AI governance: International standards to enable global coordination in AI research and development," University of Oxford, Future of Humanity Institute, April 2019, https://www.fhi.ox.ac.uk/wp-content/uploads/Standards_-FHI-Technical-Report.pdf.

275. Tim Büthe and Walter Mattli, "Typology of Global Regulation" in The new global rulers: The privatization of regulation in the world economy (Princeton University Press, 2011).

276. For example, during the 1990s, the Microsoft Windows operating system became the de facto global industry standard operating system due to its ability to leverage direct and indirect network effects. See: Tim Büthe and Walter Mattli, "Typology of Global Regulation" in The new global rulers: The privatization of regulation in the world economy (Princeton University Press, 2011).

277. "Microsoft AI powers better conversations between sellers and customers," Microsoft, February 20, 2020, https://www.microsoft.com/en-us/itshowcase/microsoft-ai-powers-better-conversations-between-sellers-and-customers.

278. "Finance uses anomaly detection and automation to transform royalty statements processing," December 6, 2019, https://www.microsoft.com/en-us/itshowcase/finance-uses-anomaly-detection-and-automation-to-transform-royalty-statements-processing.

279. "Driving Microsoft's transformation with AI," Microsoft, accessed August 27, 2021, https://www.microsoft.com/en-us/itshowcase/driving-microsofts-transformation-with-ai#primaryR6.

280. Ruchir Puri, "IBM research pioneers technologies behind new AI for IT capabilities," IBM, May 5, 2020, https://www.ibm.com/blogs/research/2020/05/ibm-research-pioneers-ai-for-it-capabilities/.

281. Cem Dilmegani, "Google is AI first: Top 15 AI projects powering Google products," AI Multiple, updated July 4, 2021, https://research.aimultiple.com/ai-is-already-at-the-heart-of-google/.

282. Alex Engler, "How open-source software shapes AI policy," The Brookings Institution, August 10, 2021, https://www.brookings.edu/research/how-open-source-software-shapes-ai-policy/.

283. "AI Fairness 360," IBM Research Trusted AI, accessed August 27, 2021, https://aif360.mybluemix.net/; "AI Explainability 360," IBM Research Trusted AI, accessed August 27, 2021, https://aix360.mybluemix.net/.

284. Tim Nicholas Rühlig, "Technical standardization, China and the future international order," Heinrich Boll Stiftung, February 2020, https://eu.boell.org/en/2020/03/03/technical-standardisation-china-and-future-international-order; William Morrissey and John Givens, "The measure of a country: America's wonkiest competition with China," Texas National Security Review, War on the Rocks, August 21, 2020, https://warontherocks.com/2020/08/the-measure-of-a-country-americas-wonkiest-competition-with-china/.

285. John Seaman, "China and the new geopolitics of technical standardization", Notes de l'Ifri, January 27, 2020, https://www.ifri.org/en/publications/notes-de-lifri/china-and-new-geopolitics-technical-standardization.

286. Tim Nicholas Rühlig, "Technical standardization, China and the future international order," p. 11, Heinrich Boll Stiftung, February 2020, https://eu.boell.org/en/2020/03/03/technical-standardisation-china-and-future-international-order.

287. Huw Roberts, et al., "The Chinese approach to artificial intelligence: An analysis of policy, ethics, and regulation, AI & Society 36, 59–77, 2021, https://link.springer.com/article/10.1007/s00146-020-00992-2.

288. "Technical Barriers to Trade Agreement," Article 2.4, World Trade Organization, accessed September 1, 2021, https://www.wto.org/english/tratop_e/tbt_e/tbt_e.htm.

289. "Technical Barriers to Trade Agreement," Article 2.4, World Trade Organization, accessed September 1, 2021, https://www.wto.org/english/tratop_e/tbt_e/tbt_e.htm.

290. Tim Büthe, "Engineers as Visionaries?" Yale Journal on Regulation, October 7, 2019, https://www.yalejreg.com/nc/engineers-as-visionaries-by-tim-buthe/.

291. Tim Büthe, "Engineers as Visionaries?" Yale Journal on Regulation, October 7, 2019, https://www.yalejreg.com/nc/engineers-as-visionaries-by-tim-buthe/.

292. Tim Büthe, "Engineers as Visionaries?" Yale Journal on Regulation, October 7, 2019, https://www.yalejreg.com/nc/engineers-as-visionaries-

by-tim-buthe/.

293. Melanie Hart and Blaine Johnson, "Mapping China's global governance ambitions," Center for American Progress, February 28, 2019, https://www.americanprogress.org/issues/security/reports/2019/02/28/466768/mapping-chinas-global-governance-ambitions/.

294. Daniel R. Russell and Blake H. Berger, "Weaponizing the Belt and Road Initiative," Asia Society Policy Institute, September 2020, https://asiasociety.org/sites/default/files/2020-09/Weaponizing%20the%20Belt%20and%20Road%20Initiative_0.pdf.

295. "The AI Act (COM/2021/206 final)," European Commission, April 21, 2021, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1623335154975&uri=CELEX%3A52021PC0206; Ursula von der Leyen, "A union that strives for more: My agenda for Europe," https://ec.europa.eu/info/sites/default/files/political-guidelines-next-commission_en_0.pdf; "White paper on artificial intelligence: a European approach to excellence and trust," European Commission, February 19, 2020, https://ec.europa.eu/info/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en.

296. Russell T. Vought, "Memorandum for the heads of executive departments and agencies," Executive Office of the President, Office of Management and Budget, November 17, 2020, https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-06.pdf.

297. "Transforming Singapore through technology," Smart Nation Singapore, accessed September 1, 2021, https://www.smartnation.gov.sg/.

298. GPAI Steering Committee," Guidance for the development of the 2022 Work Plan for Projects" (June 2021).

299. "AI for good," International Telecommunications Union, accessed September 1, 2021, https://aiforgood.itu.int/.

300. "CLAIRE receives broad mandate and funding for shaping 'AI made in Europe,'" Confederation of Laboratories for Artificial Intelligence Research in Europe, March 13, 2020, https://claire-ai.org/wp-content/uploads/2020/03/CLAIRE-Press-Release-12-2.pdf.

301. "John F. Kennedy moon speech—Rice Stadium," National Aeronautics and Space Administration, September 12, 1962, https://er.jsc.nasa.gov/seh/ricetalk.htm.

302. "Cabinet directive on regulation," Government of Canada, 2018, https://www.canada.ca/en/government/system/laws/developing-improving-federal-regulations/requirements-developing-managing-reviewing-regulations/guidelines-tools/cabinet-directive-regulation.html.

303. "Executive order 13859: Maintaining American leadership artificial intelligence," Executive Office of the President, February 11, 2019, https://www.federalregister.gov/documents/2019/02/14/2019-02544/maintaining-american-leadership-in-artificial-intelligence.

304. See, e.g., "Guidelines for trials of automated vehicles in Australia", Australian National Transport Commission, 2017, https://www.ntc.gov.au/sites/default/files/assets/files/AV_trial_guidelines.pdf; "Making space for innovation: The handbook for regulatory sandboxes," Federal Ministry for Economic Affairs and Energy and Reallabore Testraume fur Innovation und Regulierung, July 2019, https://www.bmwi.de/Redaktion/EN/Publikationen/Digitale-Welt/handbook-regulatory-sandboxes.pdf?__blob=publicationFile&v=2; "Digital health innovation action plan," U.S. Food & Drug Administration, https://www.fda.gov/media/106331/download; Sharmista Appaya and Mahjabeen Haji, "Four years and counting: What we've learned from regulatory sandboxes," World Bank Blogs, November 18, 2020, https://blogs.worldbank.org/psd/four-years-and-counting-what-weve-learned-regulatory-sandboxes.

305. "U.S. leadership in AI: A plan for federal engagement in developing technical standards and related tools," U.S. Department of Commerce, National Institute of Standards and Technology, August 9, 2019, https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_plan_9aug2019.pdf.

306. Joshua P. Meltzer, "The Impact of Artificial Intelligence on International Trade," Brookings Institution, December 18, 2018, https://www.brookings.edu/research/the-impact-of-artificial-intelligence-on-international-trade/.

307. The AI Ethical Framework category lists selected national principles, guidelines and frameworks on AI ethics. The Council of Europe's visualization of AI initiatives provides a more comprehensive, global overview over AI ethics guidelines: "AI initiatives", Council of Europe, retrieved September 22, 2021, https://www.coe.int/en/web/artificial-intelligence/national-initiatives.

308. The AI Ethical Framework category lists selected national legislative acts and/or soft regulatory documents. A comprehensive overview can be retrieved from the OECD website: "Artificial intelligence in society," OECD, June 11, 2019, https://www.oecd-ilibrary.org/sites/cf3f3be0-en/index.html?itemId=/content/component/cf3f3be0-en; "AI governance in Japan Ver 1.0 : Interim report," Expert Group on Architecture for AI Principles to be Practiced, January 15, 2021, https://www.meti.go.jp/press/2020/01/20210115003/20210115003-3.pdf; Andrea Renda et al., "Study to support an impact assessment of regulatory requirements for the artificial intelligence in Europe," European Commission, April 2021, https://op.europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1.

309. The Data Governance category lists applicable legislation and non-binding frameworks on privacy-, IP- and cyber-specific aspects which may also apply to AI systems. Please note that this is a non-exhaustive overview and the intersection between data governance, including privacy, IP and cyber, requires further research.

310. The AI Standards category describes national priorities in the field of AI standards developments by the respective national standardization institutes.

311. "Artificial intelligence in Society," OECD, June 11, 2019, https://www.oecd-ilibrary.org/sites/cf3f3be0-en/index.html?itemId=/content/component/cf3f3be0-en; "Australia's AI Action Plan," Commonwealth of Australia, June 2021, https://www.industry.gov.au/sites/default/files/June%202021/document/australias-ai-action-plan.pdf; "Making Australia's voice heard," Standards Australia, https://www.standards.org.au/getmedia/ede81912-55a2-4d8e-849f-9844993c3b9d/1515-An-Artificial-Intelligence-Standards-Roadmap12-02-2020.pdf.aspx; "Developing standards for artificial intelligence: Hearing Australia's voice," Standards Australia, June 2019, https://www.standards.org.au/getmedia/aeaa5d9e-8911-4536-8c36-76733a3950d1/Artificial-Intelligence-Discussion-Paper-(004).pdf.aspx; Gavin Brennen, et al., "An Australian strategy for the quantum revolution," Australian Strategic Policy Institute, International Cyber Policy Centre, May 13, 2021, https://www.aspi.org.au/report/australian-strategy-quantum-revolution.

312. "Canada's Digital Charter: Trust in a digital world," Government of Canada, modified January 12, 2021, https://www.ic.gc.ca/eic/site/062.nsf/eng/h_00108.html; "Directive on automated decision-making," Government of Canada, April 1, 2021, https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32592; Andrea Renda et al., "Study to support an impact assessment of regulatory requirements for the artificial intelligence in Europe," European Commission, April 2021, https://op.europa.eu/en/publication-detail/-/publication/55538b70-a638-11eb-9585-01aa75ed71a1; "Bill summary: Digital Charter Implementation Act, 2020," Government of Canada, November 23, 2020, https://www.ic.gc.ca/eic/site/062.nsf/eng/00120.html; "CAN/CIOSC 101:2019, Ethical design and use of automated decision systems," CIO Strategy Council, updated September 2020, https://ciostrategycouncil.com/standards/101_2019/; "Canadian government commits $360 million for quantum research," HPC Wire, April 20, 2021, https://www.hpcwire.com/off-the-wire/canadian-government-commits-360-million-for-quantum-research/; https://www.ibm.com/downloads/cas/E7DGKDZP; "Driving Canada's industrial & academic eminence towards a national quantum strategy," IBM, May 2021, https://www.ibm.com/downloads/cas/E7DGKDZP.

313. "Ethics guidelines for trustworthy AI," European Commission, April 8, 2019, https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai.; "The AI Act (COM/2021/206 final)," European Commission, April 21, 2021, https://digital-strategy.ec.europa.eu/en/library/proposal-regulation-laying-down-harmonised-rules-artificial-intelligence; "Payment services," European Commission, accessed September 1, 2021, https://ec.europa.eu/info/business-economy-euro/banking-and-finance/consumer-finance-and-payments/payment-services/payment-services_en; "Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC," https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG; "The EU copyright legislation," European Commission, updated July 1, 2021, https://digital-strategy.ec.europa.eu/en/policies/copyright-legislation; https://ftp.cencenelec.eu/EN/EuropeanStandardization/Sectors/AI/CEN-CLC_FGR_RoadMapAI.pdf; "Adoption of the Council Regulation to establish the new EuroHPC JU," European Commission, July 13, 2021, https://digital-strategy.ec.europa.eu/en/news/adoption-council-regulation-establish-new-eurohpc-ju

314. "AI governance in Japan Ver. 1.0: interim report," Ministry of Economy, Trade, and Industry, Expert Group on Architecture for AI Principles to be Practiced, January 15, 2021, https://www.meti.go.jp/press/2020/01/20210115003/20210115003-3.pdf; "Social principles of human-centric AI," https://www.cas.go.jp/jp/seisaku/jinkouchinou/pdf/humancentricai.pdf; "AI utilization guidelines: practical reference for AI utilization," The Conference toward AI network society," August 9, 2019, https://www.soumu.go.jp/main_content/000658284.pdf; Overview regarding the revision of the Act in May 2018, defining the acts of unfair competition on "shared data with limited access" and providing civil remedies against the acts: "Unfair Competition Prevention Act," Japanese Ministry of Economy, Trade, and Industry, accessed September 1, 2021, https://www.meti.go.jp/english/policy/economy/chizai/chiteki/index.html; "Commitment to a free, fair, and secure cyberspace," National Center of Incident Readiness and Strategy for Cybersecurity, accessed September 1, 2021, https://www.nisc.go.jp/eng/index.html#sec2; "Large-scale AI cloud computing system 'ABCI' upgraded to 'ABCI 2.0,'" AI Bridging Cloud Infrastructure, May 10, 2021, https://abci.ai/.

315. "Model artificial intelligence governance framework: second edition," Personal Data Protection Commission Singapore, January 2020, https://www.pdpc.gov.sg/help-and-resources/2020/01/second-edition-of-model-artificial-intelligence-governance-framework ; "Singapore's approach to AI governance," Personal Data Protection Commissioner Singapore, accessed September 1, 2021, https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework; "Principles to promote fairness, ethics, accountability, and transparency (FEAT) in the use of artificial intelligence and data analytics in Singapore's financial sector," Monetary Authority of Singapore, http://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf; "Launch of AI: Accelerated initiative for artificial intelligence—an accelerated application-to-grant service for patent applications in artificial intelligence," Intellectual Property Office of Singapore, April 26, 2019, https://www.ipos.gov.sg/docs/default-source/resources-library/patents/circulars/(2019)-circular-no-2---ai2-initiative_final.pdf?sfvrsn=2; "Singapore's approach to AI governance," Personal Data Protection Commissioner Singapore, accessed September 1, 2021, https://www.pdpc.gov.sg/Help-and-Resources/2020/01/Model-AI-Governance-Framework; "Principles to promote fairness, ethics, accountability, and transparency (FEAT) in the use of artificial intelligence and data analytics in Singapore's financial sector," Monetary Authority of Singapore, http://www.mas.gov.sg/~/media/MAS/News%20and%20Publications/Monographs%20and%20Information%20Papers/FEAT%20Principles%20Final.pdf; Singapore researchers plug in to world's fastest supercomputer," HPC Wire, November 30, 2020, https://www.hpcwire.com/off-the-wire/singapore-researchers-plug-in-to-worlds-fastest-supercomputer/;

316. "Ethics, transparency, and accountability framework for automated decision-making," Central Digital and Data Office, Cabinet Office, and Office for Artificial Intelligence, May 13, 2021, https://www.gov.uk/government/publications/ethics-transparency-and-accountability-framework-for-automated-decision-making; "April 2019 - BSI's activities on Artificial Intelligence (AI)", BSI, April 2019, https://www.bsigroup.com/en-GB/about-bsi/uk-national-standards-body/news/april-2019---bsis-activities-on-artificial-intelligence-ai/; "National AI Strategy", September 22, 2021, https://www.gov.uk/government/publications/national-ai-strategy; "New strategy to unleash the transformational power of artificial intelligence," Department for Digital, Culture, Media & Sport, Department for Business, Energy, & Industrial Strategy, Office for Artificial Intelligence, The Rt Hon. Oliver Dowden CBE MP, and The RT Hon. Kwasi Kwarteng MP, March 12, 2021, https://www.gov.uk/government/news/new-strategy-to-unleash-the-transformational-power-of-artificial-intelligence; "New strategy to unleash the transformational power of artificial intelligence," Department for Digital, Culture, Media & Sport, Department for Business, Energy, & Industrial Strategy, Office for Artificial Intelligence, The Rt Hon. Oliver Dowden CBE MP, and The RT Hon. Kwasi Kwarteng MP, March 12, 2021, https://www.gov.uk/government/news/new-strategy-to-unleash-the-transformational-power-of-artificial-intelligence; "Data Protection Act 2018," https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted; "UK government announces £20M DiRAC HPC funding boost for urgent scientific research," HPC Wire, January 6, 2021, https://www.hpcwire.com/off-the-wire/uk-government-announces-20m-dirac-hpc-funding-boost-for-urgent-scientific-research/.

317. "Executive order 13960: Promoting the use of trustworthy artificial intelligence in the federal government," Executive Office of the President, December 3, 2020, https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government; "Executive order 13960: Promoting the use of trustworthy artificial intelligence in the federal government," Executive Office of the President, December 3, 2020, https://www.federalregister.gov/documents/2020/12/08/2020-27065/promoting-the-use-of-trustworthy-artificial-intelligence-in-the-federal-government; "ANSI/CTA standard: Definitions/characteristics of artificial intelligence in health care," Consumer Technology Association, February 2020, https://webstore.ansi.org/Standards/ANSI/ANSICTA20892020?_ga=2.190078184.275197380.1617826921-442081003.1617826921; https://www.nist.gov/standardsgov/ai-standards-development-activities-federal-involvement; https://www.nist.gov/system/files/documents/2019/08/10/ai_standards_fedengagement_

plan_9aug2019.pdf; "AI Standards Development Activities with Federal Involvement", NIST, October 20, 2021, https://www.nist.gov/standardsgov/ai-standards-development-activities-federal-involvement

318. The AI public investment category lists figures from government investments. Conversion rate in local currency to USD from September 22, 2021. Sources: "Artificial intelligence in society," OECD, June 11, 2019, https://www.oecd-ilibrary.org/sites/cf3f3be0-en/index.html?itemId=/content/component/cf3f3be0-en; EU: "Artificial intelligence for Europe pillar 1: investment in AI", October 2019, https://www.cep.eu/fileadmin/user_upload/cep.eu/Analysen/COM_2018_237_und_795_Kuenstliche_Intelligenz/cepPolicyBrief_COM_2018__237_COM_2018__795_Artificial_Intelligence-Pillar_1.pdf; JA: "Artificial intelligence (AI) related initial government budget in Japan from 2016 to 2018", Statista, October 13, 2020, https://www.statista.com/statistics/947277/japan-artificial-intelligence-related-government-budget/; UK: "AI Sector Deal", May 21, 2019, https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal; US: Kyle Wiggers, "AI Weekly: U.S. agencies are increasing their AI investments," September 11, 2021, https://venturebeat.com/2021/09/11/ai-weekly-u-s-agencies-are-increasing-their-investments-in-ai/.

319. The AI private investment category lists selected figures from non-governmental entities investing in AI. Sources: Zachary Arnold, Ilya Rahkovsky, and Tina Huang, "Tracking AI investment: Initial findings from private markets," Center for Security and Emerging Technology, September 2020, https://cset.georgetown.edu/publication/tracking-ai-investment/-.

320. The AI R&D investment category lists selected figures on R&D spending on AI from both governmental and/or non-governmental entities. Sources: "Measuring the AI content of government-funded R&D projects: A proof of concept for the OECD Fundstat initiative," OECD, September 2021, https://www.oecd-ilibrary.org/docserver/7b43b038-en.pdf?expires=1632346986&id=id&accname=guest&checksum=5941BDFCDB48220AFB4D255F01AD8EEF ; CA: "Canada concludes inaugural plenary of the Global Partnership on Artificial Intelligence with international counterparts in Montreal," Markets Insider, December 4, 2020, https://markets.businessinsider.com/news/stocks/canada-concludes-inaugural-plenary-of-the-global-partnership-on-artificial-intelligence-with-international-counterparts-in-montr%C3%A9al-1029866048; JA: "Japan's budget for AI to be less than a fifth of that planned by U.S. and China," Japan Times, February 25, 2018, https://www.japantimes.co.jp/news/2018/02/25/business/tech/japanese-government-spending-ai-less-20-u-s-china/; EU: "cepPolicyBrief No. 2019-10", October 2019, https://www.cep.eu/fileadmin/user_upload/cep.eu/Analysen/COM_2018_237_und_795_Kuenstliche_Intelligenz/cepPolicyBrief_COM_2018__237_COM_2018__795_Artificial_Intelligence-Pillar_1.pdf; US: "Federal AI Spending to Top $6 Billion", October 2, 2021, https://www.nationaldefensemagazine.org/articles/2021/2/10/federal-ai-spending-to-top-$6-billion; UK: "AI Sector Deal", May 21, 2019, https://www.gov.uk/government/publications/artificial-intelligence-sector-deal/ai-sector-deal.

321. "Standards development stages," IEC, accessed August 25, 2021, https://www.iec.ch/standards-development/stages.

322. "Develop standards," IEEE Standards Association, accessed August 26, 2021, https://standards.ieee.org/develop/balloting-standard/balloting.html.

323. "Develop standards," IEEE Standards Association, accessed August 25, 2021, https://standards.ieee.org/develop/gaining-final-approval/finalapp.html.

324. "About International Telecommunication Union," International Telecommunications Union, accessed August 25, 2021, https://www.itu.int/en/about/Pages/default.aspx.

325. "ITU-T study groups (study period 2017–2020)," International Telecommunications Union, accessed August 25, 2021, https://www.itu.int/en/ITU-T/studygroups/2017-2020/Pages/default.aspx .

326. "Categories," International Telecommunications Union, accessed August 27, 2021, https://www.itu.int/en/ITU-T/membership/Pages/Rights.aspx .

327. "Categories," International Telecommunications Union, accessed August 27, 2021, https://www.itu.int/en/ITU-T/membership/Pages/Rights.aspx.

328. "Standards approval," International Telecommunications Union, accessed August 27, 2021, https://www.itu.int/en/ITU-T/about/Pages/approval.aspx.

BROOKINGS

www.brookings.edu

CEPS

www.ceps.eu