Q-A Pairs - Team 3

Appendix B-1: International policy documents on AI from various countries

- **[Document 1 - Europe Union]** https://apnews.com/article/ai-act-europe-regulation-59466a4d8fd3597b04542ef25831322c

1. **What were some of the controversial points discussed during the negotiations?**
   a. Controversial points included generative AI and police use of face recognition surveillance.

2. **What are the general sentiments from civil society groups towards the political deal on the AI Act?**
   a. They gave it a cool reception, waiting for technical details and expressing concerns that it didn't go far enough in protecting people.

3. **What was a major point of contention during the negotiations, and how was it addressed?**
   a. AI-powered face recognition surveillance systems; a compromise was found after intensive bargaining.

4. **What are some criticisms or concerns regarding the AI Act?**
   a. Rights groups are concerned about exemptions, lack of protection for AI systems used in migration and border control, and loopholes that may allow developers to opt out of high-risk classifications.

5. **What additional scrutiny do the most advanced foundation models face under the AI Act?**
   a. They must assess and mitigate systemic risks, report incidents, ensure cybersecurity, and report energy efficiency.

- **[Document 2]** https://www.europarl.europa.eu/news/en/press-room/20231206IPR15699/artificial-intelligence-act-deal-on-comprehensive-rules-for-trustworthy-ai

1. **What are the penalties for non-compliance with the AI Act?**
   a. Fines range from 35 million euros or 7% of global turnover to 7.5 million euros or 1.5% of turnover, depending on the infringement and company size.

2. **What are the next steps for the Artificial Intelligence Act to become EU law?**

   a. The agreed text must be formally adopted by both the European Parliament and the Council.

3. **How does the Act intend to handle the rapid expansion and capabilities of AI systems?**
   a. By setting obligations based on potential risks and impacts, including transparency for GPAI systems and stringent obligations for high-impact models to ensure they do not present systemic risks.

4. **What is the primary goal of the Artificial Intelligence Act according to the European Parliament?**
   a. The Act aims to ensure AI in Europe is safe and respects fundamental rights and democracy while enabling businesses to thrive and expand.

5. **What types of AI applications have been banned under the new regulations?**
   a. Bans include biometric categorization systems based on sensitive characteristics, untargeted scraping for facial recognition databases, emotion recognition in workplaces and educational institutions, social scoring, and AI that manipulates behavior or exploits vulnerabilities.

- **[Document 3 - China]** https://carnegieendowment.org/2023/07/10/china-s-ai-regulations-and-how-they-get-made-pub-90117

1. **What is the main focus of China's AI regulations?**
   a. Governing recommendation algorithms, synthetically generated content, and generative AI like ChatGPT.

2. **What are the key goals of China's AI regulations?**
   a. Information control, preventing excessive price discrimination, and ensuring true and accurate training data and model outputs.

3. **What innovative approach does China use in building its AI governance framework?**
   a. Targeted regulations to build bureaucratic know-how and a series of more targeted AI regulations.

4. **What challenges do China's AI regulations pose to AI developers?**

   a. Ensuring compliance with detailed regulatory requirements, such as truth and accuracy in training data and outputs, could be technically and operationally challenging.

5. **What challenges and considerations are highlighted in regulating generative AI?**
   a. Balancing effective content control with fostering the AI industry, focusing on training data accuracy and non-discriminatory outputs.

- **[Document 4 - United Kingdom]** https://post.parliament.uk/research-briefings/post-pn-0708/

1. **Does the UK's approach to AI regulation primarily rely on new, AI-specific laws?**
   a. No, it uses existing laws enforced by existing regulators.

2. **Comparatively, is the EU's proposed AI Act more prescriptive than the UK's current AI regulatory framework?**
   a. Yes, the EU AI Act proposes specific regulations for AI, including risk levels and bans on high-risk applications.

3. **What is the UK Government's approach to AI regulation as of March 2023?**
   a. The UK adopted a 'pro-innovation' approach, largely regulating AI through existing laws and principles for safety, security, and transparency among others.

4. **What are the potential benefits and risks of using AI in public services?**
   a. AI could improve healthcare outcomes and educational resources but may also exacerbate inequalities and create barriers for digitally excluded communities.

5. **What role could AI play in enhancing or undermining democracy and public trust?**
   a. Advances in AI could affect public mistrust in content and institutions, but also engage the public with politics and electoral processes.

Appendix B2: US AI Policy Documents

- **[Document 5]** Blueprint for an AI Bill of Rights

1. **What is the Blueprint for an AI Bill of Rights?**
   a. The Blueprint for an AI Bill of Rights is a set of five principles and associated practices aimed at safeguarding the rights of the American public in the

context of artificial intelligence. Safe and effective systems, algorithmic discrimination protections, data privacy, notice and explanation, human alternatives, considerations, and fallback.

2. **How can the Blueprint be implemented?**
    a. The Blueprint is accompanied by a handbook called "From Principles to Practice", which provides detailed steps for incorporating these protections into policy and practice, ensuring that AI technologies align with our highest values. Practical Steps, Policy Recommendations, Ethical Design, Case Studies, and Stakeholder Engagement.

3. **What are several challenges and ways to mitigate them?**
    a. Broadly defined harms, resource constraints, congressional action, guideline adoption, and industry and private sector engagement.

4. **Should there be biases and issues of equity?**
    a. No, there should be algorithmic discrimination protections, data privacy, and human alternatives, considerations, and fallback.

5. **Who enforces these conditions?**
    a. Government agencies, industry self regulation, legislative bodies, and from public awareness.

- **[Document 6]** Safe, Secure, and Trustworthy Development of Artificial Intelligence

1. **What are the guiding principles?**
    a. Safety and security, transparency, fairness and discrimination, privacy and civil liberties, interagency and international cooperation, public trust and ethical use

2. **What's the role of good leadership?**
    a. Setting ethical standards, risk mitigation, and public trust and accountability.

3. **Who should be a member of the White House AI Council?**
    a. (i) the Secretary of State;
    (ii) the Secretary of the Treasury;
    (iii) the Secretary of Defense;
    (iv) the Attorney General;

(v) the Secretary of Agriculture;
(vi) the Secretary of Commerce;
(vii) the Secretary of Labor;
(viii) the Secretary of HHS;
(ix) the Secretary of Housing and Urban Development;
(x) the Secretary of Transportation;
(xi) the Secretary of Energy;
(xii) the Secretary of Education;
(xiii) the Secretary of Veterans Affairs;
(xiv) the Secretary of Homeland Security;
(xv) the Administrator of the Small Business Administration;
(xvi) the Administrator of the United States Agency for International Development;
(xvii) the Director of National Intelligence;
(xviii) the Director of NSF;
(xix) the Director of OMB;
(xx) the Director of OSTP;
(xxi) the Assistant to the President for National Security Affairs;
(xxii) the Assistant to the President for Economic Policy;
(xxiii) the Assistant to the President and Domestic Policy Advisor;
(xxiv) the Assistant to the President and Chief of Staff to the Vice President;
(xxv) the Assistant to the President and Director of the Gender Policy Council;
(xxvi) the Chairman of the Council of Economic Advisers;
(xxvii) the National Cyber Director;
(xxviii) the Chairman of the Joint Chiefs of Staff; and
(xxix) the heads of such other agencies, independent regulatory agencies, and executive offices as the Chair may from time to time designate or invite to participate.

4. **How does this paper expect to attract talent in AI?**
    a. Making it easier for noncitizens to travel to the US to work in the field, improving visa processing times, as well as as expand the categories of nonimmigrants who qualify for the domestic visa renewal program covered under 22 CFR 41.111(b) to include academic J–1 research scholars and F–1 students in science, technology, engineering, and mathematics (STEM).

5. **How does it ensure safety?**

   a. Establish appropriate guidelines as well as an AI risk management framework. This includes benchmarks for evaluating and auditing AI capabilities.

- **[Document 7]** Generative Artificial Intelligence and Copyright Law

1. **Do AI outputs enjoy copyright protection?**
   a. The question of whether AI outputs, such as images or texts, enjoy copyright protection hinges on the concept of "authorship." While the U.S. Copyright Office recognizes copyright only in works created by humans, recent lawsuits challenge this requirement.

2. **Who owns the copyright to generative AI outputs?**
   a. Depending on the interpretation, the AI may be considered the author of the work. Companies such as OpenAI "bypass most copyright questions through contract."

3. **Does the AI training process infringe on copyright in other works?**
   a. AI companies may argue that their training processes constitute fair use and are therefore noninfringing. Whether or not copying constitutes fair use depends on four statutory factors under 17 U.S.C. § 107:
   1. the purpose and character of the use, including whether such use is of a commercial
   nature or is for nonprofit educational purposes;
   2. the nature of the copyrighted work;
   3. the amount and substantiality of the portion used in relation to the copyrighted work as a
   whole; and
   4. the effect of the use upon the potential market for or value of the copyrighted work.

4. **What are some considerations for Congress?**
   a. Congress may, for example, consider legislation clarifying whether AI-generated works are copyrightable, who should be considered the author of such works, or when the process of training generative AI programs constitutes fair use. They are effectively on a wait-and-see policy.

5. **What is meant by "vicarious infringement"?**
   a. Vicarious infringement applies to defendants who have "the right

and ability to supervise the infringing activity" and "a direct financial interest in such activities." For instance the defendant claims that AI companies are vicariously liable for copyright infringement during a lawsuit against Stable Diffusion.

Appendix B-3: AI policy documents from policy think-tanks and research organizations

- **[Document 8] A comprehensive and distributed approach to AI regulation**

1. **Why is there a need for comprehensive and distributed AI regulation?**
   a. Comprehensive and distributed AI regulations are needed as algorithmic decision-making systems (ADSs) have a cross-sectoral, widespread impact in areas such as education, employment, finance, healthcare and more. However, ADSs also pose risks like erroneous data, algorithmic failures and discriminatory impact. Due to the diverse nature of ADSs, it is necessary to formulate sector-specific regulations and applications that offer flexibility rather than a centralized regulatory framework.

2. **What is the CASC approach?**
   a. A central challenge of AI governance that necessitates an application specific regulatory approach is proliferation of ADSs in socioeconomic determinations. Two key interventions, addressing this challenge, are jointly known as the "CASC Approach":
      - Allowing agencies to demand information to check and review ADSs that impact their responsibilities
      - A new regulatory instrument, the Critical Algorithmic System Classification (CASC), that allows agencies to issue and enforce regulations on ADSs

3. **What is the Critical Algorithmic System Classification(CASC)**
   a. A legal designation that can be applied to an ADS category through the federal rulemaking process, leading to legally binding and enforceable rules for that ADS category. *(Note: Directly taken as it is from text)*

4. **What are some of the advantages of the CASC approach?**
   a. Some of the advantages are as follows:
      - Enables sectoral agencies to audit and regulate ADSs within their authority

        - Addresses gaps in regulation, clarifies legal uncertainties and empowers agencies to oversee ADSs impacting critical socioeconomic determinations
        - Allows US to be recognized as an undisputed leader in trustworthy AI, leading to global business development opportunities
        - Regulatory flexibility, enables better international alignment and strengthens trade relationships

5. **What are some limitations or disadvantages of the CASC approach?**
    a. Some of the limitations/disadvantages of the CASC approach are as follows:
        - Limited by the pace of the process, and its dependence of rule making makes the process an inherently retroactive rather than proactive approach
        - A lengthy regulatory process undermines efficacy of the approach
        - Additional expertise and staff capacity required within covered agencies for effective regulation execution

- **[Document 9] [AI and Geopolitics: How Might AI Affect the Rise and Fall of Nations?]**

1. **How the United States' approach to AI is influencing the future of AI geopolitics?**
    a. Lack of government regulation for private corporations dominating the AI development landscape is a key contributor towards the overall advancement of AI technologies. However, if the US government was to take a more regulatory approach towards AI technology development, we could see significant monopolization of AI resources and talent.

2. **What is China's contribution to the advancement of AI?**
    a. China has emerged as a leading force in AI, as key Chinese organizations (Huawei, Baidu and Beijing Academy of Artificial Intelligence) announced groundbreaking achievements. These announcements are representative of China's substantial investment in AI research and strategic partnerships. Through vast data resources and collaborative approaches, China's AI landscape may be a potential threat to US's global AI power dynamics.

3. **How proliferation of big technology companies, combined with AI advancement impacts geopolitical power dynamics?**
    a. Big technology companies, operating across national boundaries, exert influence at local, national, and international levels, vastly impacting

geopolitical power dynamics by shaping consumer behavior and gathering vast amounts of data. This phenomenon has led to polarization within populations and even regime changes in some countries.

4. **What are some ways in which governments can mitigate potential threats posed by AI?**
    a. Some ways in which governments can mitigate potential threats posed by AI include:
        - Strengthening resilience to AI threats: Adopting strategies of resilience to mitigate potential threats by focusing on areas like biosecurity, countering cybersecurity threats, strengthening democratic resilience, and developing emergency response options for various threats from state, sub-state, and non-state actors.
        - Non-traditional regulatory techniques: In order to truly encapsulate the everchanging AI landscape it is important for governments to look into non-traditional regulatory frameworks like investing in publicly owned data sets for AI research, issuing challenge grants for socially beneficial AI uses, establishing uniform liability rules for developers, and setting requirements for AI assessment.
        - Funding innovation: By funding national AI resources and partnering with private sector, the government can introduce improvements in risk assessments for dealing with unexpected AI-enabled issues

5. **What are some key challenges being faced by governments for AI regulation?**
    a. Governments encounter difficulties in regulating AI due to its borderless nature, rapid pace of technological advancement, and lack of traditional chokepoints for regulation. To address these challenges, governments could adopt strategies focusing on resilience-building, expand regulatory toolboxes beyond traditional methods, partner with the private sector to improve risk assessments, and continue supporting innovation in AI.

- **[Document 10] The Path to Trustworthy AI: G7 Outcomes and Implications for Global AI Governance**

1. **What are the key themes regarding emerging technologies covered in the 2023, G7 summit?**
    a. The summit focused on responsible AI governance, aligning AI development with values like democracy and human rights, addressing potential risks

associated with AI, promoting international collaboration and interoperability in AI governance frameworks.

2. **How do international organizations and multi-stakeholder initiatives contribute to the development of trustworthy AI governance frameworks?**
    a. Organizations such as OECD and UNESCO, along with initiatives like GPAI play an integral role in developing tools, regulations, technical standards and assurance techniques for trustworthy AI. Countries can then look at these initiatives as benchmarks in establishing regulatory frameworks and allocating civil liabilities.

3. **What are some challenges associated with achieving interoperability among AI governance frameworks at the international level?**
    a. Some key challenges in achieving interoperability:
        - Varying approaches and policy instruments among countries
        - Differences in defining and assessing risks associated with AI
        - Need for ongoing discussions to align regulatory frameworks and international technical standards

4. **How can international collaboration in areas like Data Free Flow with Trust (DFFT) and agile governance contribute to fostering responsible AI development?**
    a. Collaborative initiatives like DFFT aim to enhance cross-border data flow while ensuring trust in privacy, security, and intellectual property rights. Similarly, agile governance frameworks promote multi-stakeholder involvement, agile regulatory processes, and effective enforcement mechanisms to address emerging challenges in AI governance.

5. **What role do principles such as fairness, accountability, transparency, and safety play in shaping international discussions on AI governance?**
    a. Principles such as fairness, accountability, transparency, and safety are central to international discussions on AI governance, reflecting shared values among nations. These principles guide the development of regulatory frameworks, risk assessment processes, and multi-stakeholder initiatives aimed at promoting responsible AI development and deployment.

- **[Document 11]** **The EU and U.S. diverge on AI regulation: A transatlantic comparison and steps to alignment**

Q-A Pairs - Team 3

1. **What is the U.S approach to AI risk management?**
    a. The U.S. approach to AI risk management is characterized as risk-based, sectorally specific, and highly distributed across federal agencies. It relies on a patchwork of regulatory interventions and non-binding guidance documents. While these documents outline a risk-based approach and urge agencies to consider key facets of AI risk reduction, such as using scientific evidence, enforcing non-discrimination statutes, and promoting safe AI development and deployment, federal agencies have been slow to develop the required AI regulatory plans. The Biden administration revisited the topic of AI risks through the Blueprint for an AI Bill of Rights (AIBoR), endorsing a sectorally specific approach to AI governance. However, the AIBoR is nonbinding, and its principles have not led to a consistent federal approach to AI risks.

2. **What is the EU's approach to AI risk management?**
    a. The EU's approach to AI risk management is comprehensive and multifaceted, incorporating various legislative measures and regulatory frameworks. The General Data Protection Regulation (GDPR) contains clauses related to algorithmic decision-making, including requirements for human supervision and the right to meaningful information about the logic of algorithmic systems. Additionally, the EU is enacting new legislation such as the Digital Services Act (DSA), Digital Markets Act (DMA), and the proposed AI Act. The AI Act, which is still under discussion, introduces a tiered system of regulatory obligations for different AI applications, including high-risk AI systems. It mandates standards for data quality, accuracy, robustness, non-discrimination, and human oversight, with significant fines for non-compliance. The EU's approach emphasizes transparency, accountability, and regulatory oversight across various digital environments.

3. **What is the contrast between US and EU approaches to AI risk management?**
    a. The contrast between the U.S. and EU approaches to AI risk management lies in the level of regulatory coverage, central coordination, and enforcement mechanisms. While both adopt risk-based approaches and advocate for trustworthy AI principles, the EU's approach is more centrally coordinated and comprehensive. The EU has implemented legislation like the GDPR, DSA, and DMA, and is currently developing the AI Act, which includes detailed regulatory requirements for high-risk AI systems. In contrast, the U.S. approach relies on sectorally specific regulations and

non-binding guidance, with regulatory plans developed slowly across federal agencies. Enforcement in the EU is backed by investigatory powers and significant fines for non-compliance, whereas U.S. agencies may need to pursue novel litigation without explicit legal authority to regulate algorithms. Despite some overlap in principles, the U.S. and EU approaches exhibit significant differences in regulatory scope, transparency, and enforcement mechanisms.

4. **How the EU-US are collaborating on AI risk through Trade and Technology council?**
    a. The EU and US are collaborating on AI risk through the Trade and Technology Council by engaging in projects focused on advancing trustworthy AI. These include developing common terminology, metrics, and methodologies for AI risk assessment, coordinating with international standards bodies, and piloting Privacy-Enhancing Technologies in sectors like health and medicine.

5. **What are emerging challenges in transatlantic AI Risk Management?**
    a. Emerging challenges in transatlantic AI risk management include regulatory misalignment between the EU and the US, with the EU having comprehensive platform governance acts while the US lacks similar legislation. This discrepancy poses potential conflicts for multinational digital platforms operating in both regions. Additionally, the shifting nature of AI deployment, such as the emergence of large AI models and techniques like edge and federated machine learning, raises concerns about regulatory compliance across international borders. Close collaboration and alignment are crucial to navigating these challenges effectively and ensuring the responsible development and deployment of AI technologies.

- **[Document 12]** **Opportunities and blind spots in the White House's blueprint for an AI Bill of Rights**

1. **How has the White House Office of Science and Technology Policy (OSTP) attempted to address responsible AI policy, and what challenges remain in enforcing the Blueprint for an AI Bill of Rights?**
    a. The OSTP published a Blueprint for an AI Bill of Rights outlining core principles for responsible AI use. However, challenges persist in determining how grievances will be reprimanded and if the non-binding document will prompt congressional action.

2. **Which agencies have begun to adopt the blueprint/guidelines?**
    a. The Department of Defense (DOD): Implemented Ethical Principles for Artificial Intelligence. The U.S. Agency for International Development (USAID): Developed an Artificial Intelligence Action Plan.
    The Equal Employment Opportunity Commission (EEOC): Launched an AI and algorithmic fairness initiative in partnership with the Department of Labor. The Department of Energy (DOE): Established its own office to implement guidelines. The Department of Veterans Affairs (VA): Established its own office to implement guidelines. The Department of Health and Human Services (HHS): Established its own office to implement guidelines.

3. **Why is it important for law enforcement to be fully part of the national blueprint guidance?**
    a. It's crucial to include law enforcement in the national blueprint guidance to prevent discrimination, ensure accountability, and protect civil liberties. Excluding law enforcement could perpetuate biases and hinder oversight, while incorporating them ensures that AI technologies are deployed ethically and transparently, fostering public trust and confidence.

4. **What would congressional action on the subject look like?**
    a. Congressional action on the subject would involve passing legislation to codify the principles outlined in the Blueprint for an AI Bill of Rights and expanding coverage to include law enforcement and national security. This legislation would establish enforceable guidelines for data privacy, auditing automated decisions, and ensuring accountability, addressing the challenges in enforcing criteria driven by proprietary interests and providing a credible enforcement regime.

5. **What specific sectors or domains regarding civil rights are emphasized in the blueprint?**
    a. The civil rights of interest highlighted by the blueprint primarily revolve around lending, housing, and hiring.

- **[Document 13]** **Japan’s Approach to AI Regulation and Its Impact on the 2023 G7 Presidency**

1. **Which two categories can Japan’s AI regulations be classified under?**

   a. *Regulation for AI*: Regulatory reform to promote the implementation of AI. *Regulation on AI:* Regulations to manage the risks associated with AI.

2. **What did the Ministry of Economy, Trade, and Industry (METI) state in regards to AI regulation in their July 2021 report?**
   a. They stated " "legally-binding horizontal requirements for AI systems are deemed unnecessary at the moment."

3. **What are some sector specific regulations that have been implemented in Japan?**
   a. Some sector-specific regulations implemented in Japan include the Digital Platform Transparency Act and the Financial Instruments and Exchange Act. The Digital Platform Transparency Act imposes requirements on large online malls, app stores, and digital advertising businesses to ensure transparency and fairness in transactions with business users, while the Financial Instruments and Exchange Act regulates businesses engaging in algorithmic high-speed trading, requiring registration with the government and the establishment of risk management systems.

4. **What are the two groups that have formed in terms of the G7 countries and their approaches to AI related regulations?**
   a. Two groups have emerged in terms of countries' approaches to AI-related regulations: the first group advocates for a comprehensive, binding framework focusing on governance, transparency, and security, including countries like France, Germany, Italy (under the EU AI Act), and Canada (proposing AIDA). The second group adopts a sector-specific, nonbinding guidance approach, emphasizing appropriate AI governance with a focus on transparency and data protection, represented by countries like Japan and the United Kingdom, with the United States potentially shifting towards this approach pending legislation like the Algorithmic Accountability Act.

5. **What is a possible step for collaboration amongst the G7 countries in regards to AI policy?**
   a. A relatively easy step would be to set up an AI incidents database that spans multiple countries.

- **[Document 14] Toward international cooperation on AI governance—the US executive order on AI**

1. **What is the name of the executive order released by the White House on October 30 regarding AI?**
    a. The executive order is called the Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence (EOAI)

2. **How does the EOAI contribute to U.S. leadership in AI governance?**
    a. The EOAI mobilizes the federal government to develop guidelines, principles, and reports on AI use and development, enhancing U.S. leadership in AI governance.

3. **What opportunity does Vice President Kamala Harris have regarding international AI governance?**
    a. Vice President Kamala Harris, as head of the U.S. delegation to the U.K. AI Safety Summit, has the opportunity to lead the further development of international AI governance.

4. **How are the White House Voluntary AI Commitments influencing international AI outcomes?**
    a. The White House Voluntary AI Commitments have become the basis for the International Code of Conduct for Organizations Developing Advanced AI Systems released by the G7, influencing international AI outcomes.

5. **What is the purpose of the Brookings/CEPS Forum on Cooperation in AI (FCAI)?**
    a. The FCAI focuses on identifying opportunities for international cooperation on AI, especially in light of the pace and scope of domestic AI governance mechanisms being developed globally.

- **[Document 15] Choking off China's Access to the Future of AI**

1. **What were the recent rounds of semiconductor related export controls announced by the Biden administration?**
    a. The recent round of semiconductor-related export controls announced by the Biden administration includes measures aimed at restricting China's access to advanced technologies from companies like Nvidia and AMD, blocking the sale of high-end AI chips, and limiting China's ability to design chips using U.S.-made software from companies such as Mentor Graphics, Cadence Design Systems, and Synopsys. Additionally, restrictions target semiconductor manufacturing equipment, affecting companies like SMIC

and YMTC, and aim to prevent China from developing its own equipment by restricting access to U.S.-built components.

2. **What are the criticisms of the export controls?**
    a. Critics of the export controls argue that while they aim to curb China's technological advancement, they may inadvertently harm U.S. companies and global innovation. Some contend that the restrictions could lead to reduced revenues for American chip manufacturers like Nvidia and AMD, while also potentially spurring China to accelerate its efforts to develop indigenous semiconductor technologies. Additionally, critics express concerns about the broader economic implications, including potential disruptions to global supply chains and increased tensions in U.S.-China relations. Moreover, there are fears that the controls could stifle collaboration and innovation in the semiconductor industry, ultimately hindering progress in AI and other emerging technologies.

3. **Why is the pace of adding Chinese companies to the Entity List a source of frustration for Congress and the White House?**
    a. The slow pace of adding Chinese companies to the Entity List frustrates Congress and the White House because it delays the implementation of policies aimed at restricting Chinese access to critical technologies, such as AI chip design and semiconductor manufacturing equipment.

4. **What are some notable Chinese AI chip design companies mentioned in the text?**
    a. One notable Chinese AI chip design company mentioned in the text is Cambricon.

5. **Why is the inclusion of Chinese chip design companies on the Entity List significant?**
    a. The inclusion of Chinese chip design companies on the Entity List is significant because it restricts their access to certain technologies and limits their ability to conduct business with entities in the United States, affecting their operations and growth potential.

Appendix B-4: AI policy documents from international organizations

- **[Document 16 - United Nations]** https://www.un.org/techenvoy/sites/www.un.org.techenvoy/files/ai_advisory_body_interim_report.pdf

Q-A Pairs - Team 3

1. **What are some examples of opportunities for AI? Give a brief description/explanation of each.**
    a. People-assistive AI, sectoral opportunities, scientific opportunities, public sector opportunities, etc.

2. **What are some examples of risks of AI caused by humans?**
    a. Deep fakes and hostile information campaigns

3. **Other than misuse, what is another challenge of AI?**
    a. Missed uses - failing to take advantage of and share the benefits of AI technologies out of an excess of caution.

4. **For AI governance principles drafted in this report, which existing institutions did the report refer to?**
    a. FATF, FSB, IAEA, ICANN, ICAO, ILO, IMO, IPCC, ITU, SWIFT and UNOOSA

5. **In which instances can the UN act as the arbiter of AI governance? How?**
    a. Challenges to international security - help ensure that there are no accountability gaps, for example by encouraging states to report analogous to reporting on the SDGs targets and the Universal Periodic Review that facilitates monitoring, assessing, and reporting on human rights practices

- **[Document 17 - OECD]** https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449

1. **What is the purpose of the development of this Recommendation?**
    a. to set a standard that is implementable and flexible enough to stand the test of time in a rapidly evolving field.

2. **What are the principles for responsible stewardship of trustworthy AI?**
    a. Inclusive growth, human-centered values and fairness, transparency and explainability, robustness, security and safety, and accountability

3. **How should AI actors ensure robustness, security, and safety?**
    a. Ensure traceability, employ risk management approach to each phase of the AI system lifecycle

4. **What are some recommendations for the government regarding building human capacity?**

    a. Empower people to effectively use and interact with AI systems, equip them with necessary skills, ensure a fair transition for workers, enhance safety of workers and the quality of jobs

5. **What are some recommendations for the government regarding international cooperation for trustworthy AI?**
    a. Foster the sharing of AI knowledge internationally, encourage development of internationally comparable metrics

- **[Document 18 - World Bank]** https://documents1.worldbank.org/curated/en/487931621237422984/pdf/Harnessing-Artificial-Intelligence-for-Development-on-the-Post-COVID-19-Era-A-Review-of-National-AI-Strategies-and-Policies.pdf

1. **What is the role of the private sector?**
    a. Innovation, development and application of AI in the digital economy.
    b. diffusion of AI technology on the supply side, and adoption and usage of AI on the demand side.

2. **What are the eight policy domains within AI strategies?**
    a. scientific research, AI talent development, entrepreneurial ecosystem, standards for ethical or trustworthy AI, data access, AI adoption in the public sector, strategic sectoral targeting of AI, building capabilities for AI governance

3. **What were some strengths and weaknesses of Finland?**
    a. Strength: advanced digital economies
    b. Weakness: lacks economies of scale, internationally connected companies and foreign direct investment, and exhibits slow commercialization.

4. **How was the role of government in the Finnish and UAE National AI strategies similar and different?**
    a. Similar: active roles in developing and executing AI policies and initiatives - expansion of AI in public service, developing local scientific research capabilities, and developing AI training programs for students and government employees through public-private partnerships.
    b. Different: While the UAE has taken a hybrid approach with more top-down directed initiatives to accelerate the development of an AI ecosystem, Finland has instead exhibited a mostly bottom-up approach. Other key

differences include the greater focus the UAE has had on acquiring AI talent from abroad, as well as their more emphatic role in directing the sectoral adoption of AI.

5. **What do India and China both focus on enabling?**
   a. Technological development

Appendix B-5: Comprehensive AI Public Policy Forums and Repositories

- **[Document 19] The end of the Affordable Connectivity Program is almost here, threatening to widen the digital divide**

1. **What is the affordable connectivity program and is it ending soon?**
   a. Affordable Connectivity Program (ACP) was enacted as part of the 2021 Infrastructure Investment and Jobs Act on the basis that “a broadband connection and digital literacy are increasingly critical to how individuals participate in the society, economy, and civic institutions of the United States; and access health care and essential services, obtain education, and build careers.” The program which provides a $30 per month subsidy for broadband to about 23 million homes is likely to run out of funds sometime in late April or May 2024.

2. **Why wouldn’t congress extend the Affordable Connectivity Program (ACP)?**
   a. The first reason is that legislators will not vote for an extension unless the program is changed to limit eligibility and costs. The second, and likely larger challenge, is that while the majority of Democrats and Republicans support an ACP extension, current Republican House leadership is following the “Hastert Rule” by which the Republican Speaker will not allow legislation to be voted on unless the majority of Republicans support it.

3. **What is the importance of the Affordable Connectivity Program?**
   a. There is a great cost to society for “digital exclusion.” These costs are well documented and include increasing the cost to provide government services, lower literacy rates, and decreased economic growth. Furthermore, lack of access to quickly evolving artificial intelligence technology could drive an even larger gap especially in education and healthcare.

4. **Which elected officials have actively supported the Affordable Connectivity Program (ACP)?**

   a. Elected officials from the Democrat party broadly support the ACP. In the house there are 12 Republican co-sponsors and in the Senate conservative Republican Senator J.D. Vance (R-Ohio) and Senator Kevin Cramer (R-N.D.) have supported the bill. Furthermore, 26 governors from both parties signed a letter endorsing the extension of the program.

5. **Is access to the internet important for healthcare?**
   a. Yes, especially when it comes to telehealth. A recent study found that using telehealth for patients with cancer ranged from $147 to $186 per visit. Another study found that veterans who utilized a new tele-emergency service were nearly half as likely to visit an emergency department in-person and showed reduced short-term Veteran visits to emergency departments outside of VA.

- **[Document 20] AI Orders and Summits and Forums, Oh My!**

1. **Can you tell me about the new Executive Order on AI that Joe Biden is signing?**
   a. The Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence is a first-of-its-kind executive action to quickly establish oversight of the rapidly evolving technology while Congress works to develop a comprehensive regulatory framework. The document is devoted, in large part, to national security concerns, doling out various new responsibilities to the Secretaries of Defense and Homeland Security, the Director of National Intelligence, and other agencies.

2. **What are the main parts of the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence?**
   a. Creating new safety and security standards for AI
   Protecting consumer privacy
   Protecting consumers overall by evaluating potentially harmful AI-related health-care practices
   Supporting workers
   Promoting innovation and competition
   Working with international partners to implement AI standards globally
   Developing guidance for federal agencies' use and procurement of AI
   Advancing equity and civil rights by creating guidance and research that avoids further algorithmic discrimination

3. **How does the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligencespecifically address fake AI generated content?**
    a. They secured voluntary commitments from Anthropic, Google, OpenAI, to clearly label all AI-generated content. It also required the Department of Commerce to develop guidance for labeling AI-generated content.

4. **What have leaders said about the signing of the Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence?**
    a. Senate Majority Leader Charles Schumer (D-NY) congratulated the President on this "crucial step" to ensure the US remains a leader of AI innovation, but warned that more is needed. "All executive orders are limited in what they can do, so it is now on Congress to augment, expand, and cement this massive start with legislation." The National Science Foundation (NSF), an independent government agency that's also the primary investor in non-defense AI research, also embraced the Executive Order. "NSF stands ready to fully implement the actions outlined in today's Executive Order as well as the eight guiding principles and priorities it lays out."

5. **How are countries addressing frontier AI?**
    a. The UK Department of Science, Technology, and Innovation created a "Frontier AI Taskforce" to keep a pulse on bleeding edge AI developments. This group has issued multiple reports and since its founding in September 2023 the group has tripled its research capacity, cemented new partnerships with leading AI organizations, and supported the development of Isambard-AI, an AI supercomputer where more intensive safety research will be conducted, among other developments.

- **[Document 21]** Secure, Governable Chips

1. **What are the primary national security risks associated with AI and advanced computing as outlined in the document?**
    a. AI systems could be used by irresponsible actors to enable mass surveillance, conduct cyberattacks, and design novel biological weapons.

2. **How might the implementation of on-chip governance mechanisms impact the global competitiveness of U.S. firms in the AI and semiconductor industries?**

a. Given that on-chip governance mechanisms need to be implemented on commercial chips, much of the necessary R&D will need to happen in an industry setting. To incentivize this work, the DoC should consider making commitments related to future access to export markets to U.S. chip firms, conditional on firms implementing a specific set of security features on controlled products. Such commitments would be an effective way of incentivizing the necessary R&D without spending public money, given the large amount of lost revenue to chip firms caused by export restrictions.

3. **What are some examples of current applications of on-chip mechanisms in various technologies as mentioned in the report?**

    a. On the iPhone, on-chip mechanisms ensure that unauthorized applications can't be installed. Google uses on-chip mechanisms to remotely verify that chips running in their data centers have not been compromised.

4. **Considering the ethical implications, how could on-chip governance mechanisms balance the need for security with user privacy and rights?**

    a. On-chip governance is better implemented through privacy-preserving "verification" and "operating licenses" for AI chips used in data centers. "Verification" involves the user of a chip making claims that are verifiable by another party about what they are doing with the chip. For example, verifying the quantity of computation or the dataset used in a particular training run.[5] Secure on-chip verification of this kind is made possible by a "Trusted Execution Environment" (TEE). Because of the TEE's security properties, the verifier can trust that information received from the TEE has not been "spoofed," without the chip's user needing to divulge sensitive data.[6] "Operating licenses" provide an enforcement mechanism. This is useful in cases where, for example, the chip's owner is found to have acquired the chip in violation of an export control agreement, or if the chip's user refuses to participate in a legally required verification process.

5. **What are the proposed stages for the development and rollout of on-chip governance for data center AI chips?**

    a. In the short term, firmware updates could be deployed to exported AI chips implementing early versions of a hardware operating license linked to the terms of an export license. This would be useful as an additional cautionary measure for already-planned AI chip exports to high-diversion-risk geographies. A promising and relatively feasible next step would be to make devices "tamper-evident" (attempts to tamper with the chips would leave indelible evidence). This could be a sufficient level of security in cases where occasional physical inspections of the hardware are possible. For subsequent generations of AI chips, hardware security features could be further hardened, working toward full “tamper-proofing” to make physical inspections less necessary.