Comparing AI Regulation Frameworks: The EU, US and China (Working Title)

3 May 2024 9:39 pm EST

I’ve been working almost 4 weeks F/T researching and writing this paper trying to follow our original plan: a simple paper that reuses most of the content from the original LaTeX followed by a more fleshed out one. This is the simple version of the paper which focuses on comparing the core 3 AI frameworks.

I spent this week trying to add open-source and explain the evolving dynamics in AI regulation due to rapid growing economic competition and geopolitical tensions between the US-China (and to a much lesser extent EU-China e.g. EV car tariffs and heavy German energy-intense industry moving to China due to ~3x increase in German energy and 30% discount in already cheap China energy). This cannot be done in a through, well-researched, and parallel comparative fashion without increasing the original LaTeX paper several-fold so I pulled this content for a longer-form paper.

We can get this paper out almost immediately with updates to the EU section that include citations. Alternatively, we can fold this into the larger paper I’ve been working on that elaborates upon the open-source, goes into much more detail on US AI regulations beyond just EO #14110, and future trajectories of AI regulation arising from growing trade imbalances/geopolitical tensions.

We should pick between on of these two scenarios for the immediate paper(s)

**Scenario A: (the 2nd longer paper might be tricky since we have to be careful to avoid self-plagiarism with content from first short paper)**

First Short put this short paper with only “Overview” and minimal “Laws and Regulations” sections preserving the core of the original LaTeX paper out on ArXiv.org

* Christian Schroeder: The European Union
* Kathrine L. Elkins: The United States
* Jon Chun: China

Followed by long paper with full/expanded (new sections added since LaTex, more text and tables not included in this doc, e.g. sections on US Congress, State, Local regulations, etc) for SSRN or such.

* Jon Chun: China, The United States
* Christian Schroeder: The European Union
* Kathrine L. Elkins: The United States

**Scenario B:**

Just one long paper will full/expanded (no first short paper) for SSRN or such

* Jon Chun: China, The United States (The US Section is longer and more detailed than China + EU together)
* Christian Schroeder: The European Union
* Kathrine L. Elkins: The United States

There are several post NeurIPS papers I’ve done research for in the policy, risk management/audit and industrial policy space we can talk about later.

TODO:

1. Christian looks at Jon’s notes for EU section
2. Figure out what to do about narrative (i.e.)EU is it somewhat like China re pragmatism and enforcement on the ground
3. Kate and Jon review Christian’s comments on US section. Edit and add updates
4. Kate expands on the US Open-Source section, update and relevance to current AI regulation
5. Jon expands and updates Geopolitical Tensions Section (and harmonizes with the introduction on geopolitical situation)
6. Jon revise the Conclusion to tie together 3 themes
   1. Comparison 3
   2. OSS
   3. Dynamic changes with US-China tensions
7. Christian adds some moderating to abstract and elsewhere (Kate will also work on this)
8. Jon adds citations
9. Kate checks larger group paper section on regulation(both versions)DONE
10. Think about open-source as a focal point
11. Check Jon’s description of open source with the beginning of open source in overleaf
12. Harmonize the intro

==================================================

Updates and Corrections to Existing Sections

==================================================

Paper Notes:

Color Codes:

Blue : add citation

Red: edit, delete, or add text

+

### **ABSTRACT**

As a powerful and rapidly advancing dual-use technology, AI offers both immense benefits and worrisome societal risks. In response, governing bodies around the world are developing a range of regulatory AI laws and policies. This paper compares three distinct approaches taken by the EU, the US, and China who together comprise the leaders in both AI innovation and AI regulation that influence the broader international community. Each of these three emerging regulatory systems reflect distinct cultural, political and economic perspectives and highlight differing regional perspectives on regulatory risk-benefit tradeoffs. These differing frameworks embed divergent judgments on the balance between safety versus innovation and cooperation versus competition. They also reflect differing stances in regards to trust in centralized authority versus trust in decentralized free market of self-interested stakeholders.

### **INTRODUCTION**

At the eve of November 29th, 2022, governments around the world were making steady progress in drafting regulation on AI. Following the 2021 regulations on recommendation algorithms, several Chinese government ministries had just jointly released regulations on deepfakes on November 25th. The Biden government had published its Blueprint for an AI Bill of Rights in October, speaking of the need to protect citizen's privacy and freedom from algorithmic discrimination. In the same month, the EU's Digital Services Act, now augmented with provisions against AI-generated disinformation, had come into effect. Meanwhile, the general orientation of the EU AI Act, a comprehensive common regulatory and legal framework for AI-related risks proposed by the EU Commission in April, was now being actively worked out.

Underlying these varicolored global efforts was an almost universal acknowledgement of the centrality of AI-driven algorithms within the digital economy and the importance of the latter to national economies at large. The 2020 US elections had catalyzed global concerns surrounding AI-generated disinformation and election integrity, including the role of content recommendation systems in social media. The rise of TikTok, reaching over 2 billion global users by October 2022, had helped fuel Chinese government efforts to regulate social media in line with ``core socialist values''. At the same time, China had become concerned about issues surrounding transparency, privacy, and workers' rights, echoing simultaneous dynamics within the EU and US. Global opinion within the latter had been shaped by popular analyses estimating as many as half of US jobs at risk of automation.

### **UPDATES/EDITS to original doc**

P3/C2/L161:

Growing economic threat

P4/C1/167:

INSERT new paragraph:

Concern over China’s growing economic in strategic technologies outlined in their China 2015 report and commercial dominance worldwide via the Belt and Road Initiative.

P4/C1/L167:

Factual error: 24 Feb 2022 Russia invades Ukraine (18 mos later) 31 Aug 2023 US restricts NVIDIA/AMD chips to some Middle East countries

P4/C1/L184-187:

Closed-closed:

INSERT (after) a paragraph describing the criteria, members and controversy around those invited as Frontier Model providers

P4/C1/L217:

Explain/contrast US model prioritizing market mechanisms, self-regulation, etc

INSERT: Concerns with regulatory capture, lobbyist, ROI

Incident of OpenAI Altman lobbying for strict US regulation at same time open EU regulation as logical profit maximizing strategy corp-govt

P4/C2/L165-183:

EXPAND INTO SECTION “Multi-Level US AI Regulation”

INSERT Fig.Unified AI Regulation Timeline

* [[2402.05048] How VADER is your AI? Towards a definition of artificial intelligence systems appropriate for regulation (arxiv.org)](https://arxiv.org/abs/2402.05048)

P4/C2/L204:

UPDATE to add final approval and enforcement start date

P5/C1/L244:

INSERT BEFORE: Fig: Canonical EU AI Act Use-Case Risk Pyramid

P5/C1/L249:

Refer to Fig Use-Case Risk Pyramid

P5/C2/L245:

Clarify this statement

P5/C2/L248:

INSERT Table that enumerates all the exemptions with clarifying notes (Key info)

P5/C2/L251:

Update from LEAKED to actual to verbage/interpretation from final version

P5/C2/L265:

Update from LEAKED to actual verbiage/interpretation from final version

P6/C1/L278:

INSERT figure illustrating value chain, responsible parties, and regulatory pre-release/reporting/monitoring requirements

P6/C1/L282:

Does the final version somewhat resolve this ‘confusion’

P6/C1/L301:

Unclear to what extent this applies to open-source AI given they, like PCs, are general purpose computing/cognitive devices

P6/C1/L311:

Has the EU determined that GenAI trained on copyrighted works violate IP law? Undetermined in the US

P6/C1/L327:

UPDATE from LEAKED to final passed version with current interpretation

P6/C2/L281:

UPDATE this entire section to comport with final version

P6/C2/L300:

Confirm the final version agrees with facts/opinions in this section

P6/C2/L322:

Transatlantic agreement only apply to US-EU, not EU-rest of the world

What happens if EU becomes like China where citizen evade EU restrictions by using real-time VPNs or simply batch process data with AI offshore and only import the results diluted by some Human in the Loop mitigation workflow? Overseas subsidiaries, etc.

P6/C2/L328:

UPDATE with final version, fact check, and verify opinions on France, Germany and UK stances on final version

P7/C1/L343:

UPDATE with the final version and latest on harmonized standards

P7/C1/L350:

### **1. AI Governance**

#### **1.1. Overview**

This section describes the emerging AI regulatory frameworks in the EU, US, and China. In particular, it contrasts the top-down, universal risk-based approach of the EU AI Act with the more market-driven approach of the US that emphasizes coordinating existing legal, regulatory, and enforcement entities from the federal level down. In between is the Chinese approach that has the appearance of centralized regulatory control, yet in practice emphasizes diffuse innovation and economic development at the local levels like the US.

While the EU and China appear to have relatively stable AI regulatory frameworks, there is a growing debate in the US about the future direction. The Biden Executive Order #14110 on Safe, Secure, and Transparent Development and Use of AI coordinates over 100 specific tasks to over 50 federal entities in a decentralized way that largely augments existing regulatory laws and agencies. However a number of US Congressional committees, proposals, and influential public/corporate interest groups are lobbying for a new AI regulatory structure more centralized, restrictive, and punitive than EO #14110 including some requiring centralized registration of models, proofs of AI safety, and criminal penalities (LegiScan 2024, Schumer 2023).

#### **1.2. Open Source AI**

Despite its propensity for comprehensive legal frameworks, Europe-wide legislation on open source was missing by November 2022, despite a 2018 European Commission's landmark study estimating it annually creating \euro{}65-95bn of revenue across the Union and identifying open source software and hardware as a ``public good''. Nevertheless, the European Commission played a central role in fomenting the member states' individual efforts at open source regulation. Starting from 2000, the European Commission enacted an Open Source Strategy aiming at supporting the open source ecosystem pertaining to software internally used by EU institutions. Initially concerned with the adoption of open source software such as Linux and Apache Web Server, the OSS eventually gave rise to an open source software observatory, and even the EU's institutions' own open source software license. Over time, open source software became the preferred solution for new software developments, including e-government software. After the discovery of the OpenSSL Heartbleed bug in 2014, the European Commission intensified its engagement with open source communities, funding bug bounty programmes, hackathons, conferences through their Free and Open Source Auditing (FOSSA) initiatives and starting its inaugural Open Source Software Strategy in 2017. This eventually led to the establishment of the European Commission's own Open Source Programme Office (OSPO), a dedicated department driving the Commission's own open source strategy, with the ambition to open source all software used in the Commission's own institutions. By January 2022, the European Commission's OSPO had announced its first bug bounty program, providing a de-facto succession of its FOSSA initiatives. By November 29th, 2022, the European Commission had long decided to ``lead Europe's digital transition by example'', benefiting ``start-ups, innovators, citizens and public administrations by open sourcing its software solutions'', and spurring innovation ``thanks to publicly available [] Commission code''.

Among European countries, by November 2022 open source software had had the most economic impact on the French economy, representing a market of an estimated size of \euro{}6bn, followed closely by the UK and Germany, in the latter of which an estimated 7 out of 10 companies were using open source software. Citing the contributions of open source software to ``innovation, technological independence and a more ethical and responsible digital environment'', leading French industry interest group CNLL expected further rapid growth of the open source sector, and called on the public sector to adopt more pro-active procurement strategies, dedicated funding, and pro-competitive measures that ``limit the ability of dominant players to lock in the market to the detriment of SMEs''. Such demands resonated with calls to harness the potential of open source to counter ``risks of economic subjugation, geostrategic and technological dependence'', and to achieve ``digital souvereignty'' and ``democratic trust'' in line with ``European values''.

### **2. United States**

(INSERT MODIFIED: 2.1.The US Regulatory Landscape)

#### **2.1. Overview**

On October 30, 2023 US President Biden signed an executive order (EO #14110) on the Safe,Secure,and Trustworthy Development and Use of Artificial Intelligence [cite]. This act moved beyond the voluntary commitments secured in July 2023 (Whitehouse 2023a) and the Blueprint for an AI Bill of Rights (Whitehouse 2022) released in October 2022. On April 29th The White House announced that federal agencies had completed all of the key actions mandated by the 180-day timeline pertaining to the order. (Whitehouse 2024b). EO #14110 represents the most comprehensive form of AI regulation in the United States, directly delegating over 50 existing federal regulatory agencies and other bodies with over 100 specific tasks to build out the capacity to incorporate emerging concerns due to AI.

#### **2.2 Laws and Regulations**

EO #14110 represents somewhat of a departure from the more typical US approach to regulation. In the US, the legislative branch typically passes laws that form the framework for regulation, which are then enforced by the executive branch, primarily under the oversight of various federal agencies. For example, the US Congress passes laws that define specific industries or activities along with broad goals such as advancing scientific research (National Science Foundation), promoting fair markets (Securities and Exchange Commission), and safeguarding the environment (Environmental Protection Agency). At times, multiple agencies will be tasked with regulating different aspects of the same broad goal. For example, the Federal Trade Commission (FTC), the Consumer Product Safety Commission (CPSC), and the Consumer Financial Protection Bureau (CFPB) specialize in different aspects of consumer protection and safety.

The rapid pace of AI innovation, the lack of technical expertise in government, and the immense potential impact of AI has reversed this normal sequence for enacting regulation. Instead, EO #14110 begins with the executive branch rather than the legislative branch. Nonetheless, aspects of the executive order reflect a distinct approach that can be characterized as “bottom-up” rather than “top-down.” In contrast to the more centralized, top-down approach to AI regulation prioritizing safety (European Parliment 2016) and social stability (China), the United States has traditionally taken a more distributed, multi-stakeholder approach to regulation. While universal directives on AI are provided by the ultimate source of authority in the centralized political bodies of the CCP, and to a lesser extent, the European Commission, a wide range of guidelines, initiatives, laws, and other policies including trade related to AI are distributed between various US federal branches, agencies and even states. This philosophical distrust of centralized power is reflected in the very design of the American system of checks and balances between branches of government. The decentralized US approach is also a way to reduce bureaucratic layers, more directly empower domain experts, and balance power between competing narrow, self-interested parties. This includes powerful voting blocks, special interests, and $46 billion dollar state and federal lobby industry (Massoglia 2024).

Commercial applications of technology within the US are regulated through various mechanisms including legislative action, executive orders, agency rulemaking, industry self-regulation, international agreements, and private self-regulation. Typically, Congress begins the process by passing laws setting broad requirements, which are then used by executive branch agencies like the DOC, FDA, or EPA as the basis for developing more detailed regulations. The President can also initiate regulation through executive orders. US States and municipalities can also add regulations in areas they feel federal regulations are inadequate or missing like in environmental, labor or privacy requirements. Standards and guidelines have evolved for movie ratings, medical practice, real estate transactions, and other commercial practices to self-regulate their own industry. To remain competitive in rapidly changing world markets, US tech companies have often pursued this self-regulation strategy in terms of privacy, digital advertising, content moderation, and cybersecurity. Furthermore, international agreements or regulations are sometimes adopted by US companies to do business abroad like the EU GDPR (European Parliament and Council of the European Union 2016) and China’s Cybersecurity Law (National People's Congress of the People's Republic of China 2016). The regulatory process often combines these approaches, with laws providing the foundation for agency regulations, involving public input, expert consultation as well as revision as technologies and circumstances evolve.

EO #14110 is a case where the executive branch is initiating many AI-related policies--from research to regulation--partly due to its ability to more quickly respond in a coherent and comprehensive manner. Although somewhat exceptional for the US process of lawmaking, Whitehouse Presidential executive orders more closely match the top-down, centralized organization of the European Commission in Brussels and the CCP in Beijing. However, EO #14110 organizes a distributed regulatory system wherein specific objectives with deadlines are being delegated to various federal agencies directly from the executive branch. Meanwhile, the US legislative branch is considering dozens of individual bills (GoveTrack 2023). Two notable, ambitious, and more restrictive plans have been introduced by Senator Schumer in the form of his SAFE initiative (Schumer 2023) and the Blumenthal-Hawley Framework (Blumenthal 2024). Finally, individual US states and municipalities have also passed laws and are debating more extensive regulation regarding AI (IAAP 2024). Given the general supremacy of federal laws and regulations in the US and to stay focused on comparing the national policies with the EU and China, this paper focuses on the coherent and comprehensive national framework laid out by EO #14110.

#### **2.3 Whitehouse Executive Order 14110**

Since 2016 and over three different Presidential administrations, a number of executive orders related to AI have been issued. The Biden Whitehouse’s October 2023 “Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence” is the most comprehensive to date (Whitehouse 2023b). It directs over fifty federal agencies to take over 100 specific actions addressing eight core policy areas listed in Table.ZZ below including: safety and security, innovation and competition, worker support, bias and civil rights, consumer protection, privacy, federal use of AI, and international leadership (Whitehouse 2024a). The eight policy areas are ranked by the aggregate number of requirements and federal entities engaged in each area arguably providing a loose guidance on the relevance of each policy areas from the most (federal use, safety/security, and innovation/competition) to least (workers support) to those in between (the rows in gray). This implements many guidelines in the 2022 AI Bill of Rights to ensure the responsible design and use of artificial intelligence to protect civil rights and privacy in areas such as hiring, healthcare, and surveillance (Whitehouse 2022).

This EO #14110 on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence addresses many of the core concerns highlighted in the EU AI Act but does so with several key differences (CRS 2024). First, the EU AI Act establishes a new regulatory agency, the EU AI Office, that coordinates with member states, industry and civil society, while current US strategy relies upon augmenting the extensive network of existing US federal agencies with pre-existing specialized domain expertise. Secondly, because the US approach involves over fifty federal agencies, it is much more extensive in implementation details than the EU. It also directly addresses broader issues like unemployment, education, research, and consumer protection. Third, again in contrast to the EU AI Act, this US strategy is arguably more immediately actionable given the over one hundred specific objectives with most deadlines delegated to federal agencies to be completed within 180 to 270 days. These agencies are already specialized across a broad spectrum of existing federal government responsibilities that are being disrupted by AI. The US approach can be seen to emphasize extending expansive regulatory and legal frameworks from the ground up where infrastructure already exists, in contrast to creating new central regulatory framework.

| **Relevance** | **Policy Area** | **Requirements/Entities** | **Federal Entities \*** |
| --- | --- | --- | --- |
| **H**  **I**  **G**  **H** | Federal use of AI | 29 requirements  40 entities | OMB, OPM, CFO, GSA, etc. |
| Safety and security | 27 requirements  30 entities | NIST, DOE, DOC, SRMA, Treasury, DHS, DOD, etc. |
| Innovation and competition | 21 requirements  10 entities | DOS, DHS, DOL, NSF, USPTO, HHS, VA, DOE, PCAST, OSTP+ |
| **M**  **E**  **D**  **I**  **U**  **M** | Consideration of AI bias and civil rights | 9 requirements  8 entities | DOJ, OPM, HHS, USDA, DOL, HUD, DHS, OSTP |
| Consumer protection | 9 requirements  5 entities | HHS, DOT, ED, DOD, VA |
| Privacy | 6 requirements  9 entities | OMB, NIST, NSF, FPC, ICSP, DOJ, CEA, OSTP, DOE |
| International leadership | 6 requirements  7 entities | DOC, DOS, USAID, DHS, NIST, DOE, NSF |
| **L**  **O**  **W** | Worker support | 4 requirements  2 entities | CEA, DOL |

**Fig.ZZ** Executive Order #14110 on the Safe, Secure, and Trustworth Development and Use of AI

(\* see Appendix A agency acronyms)

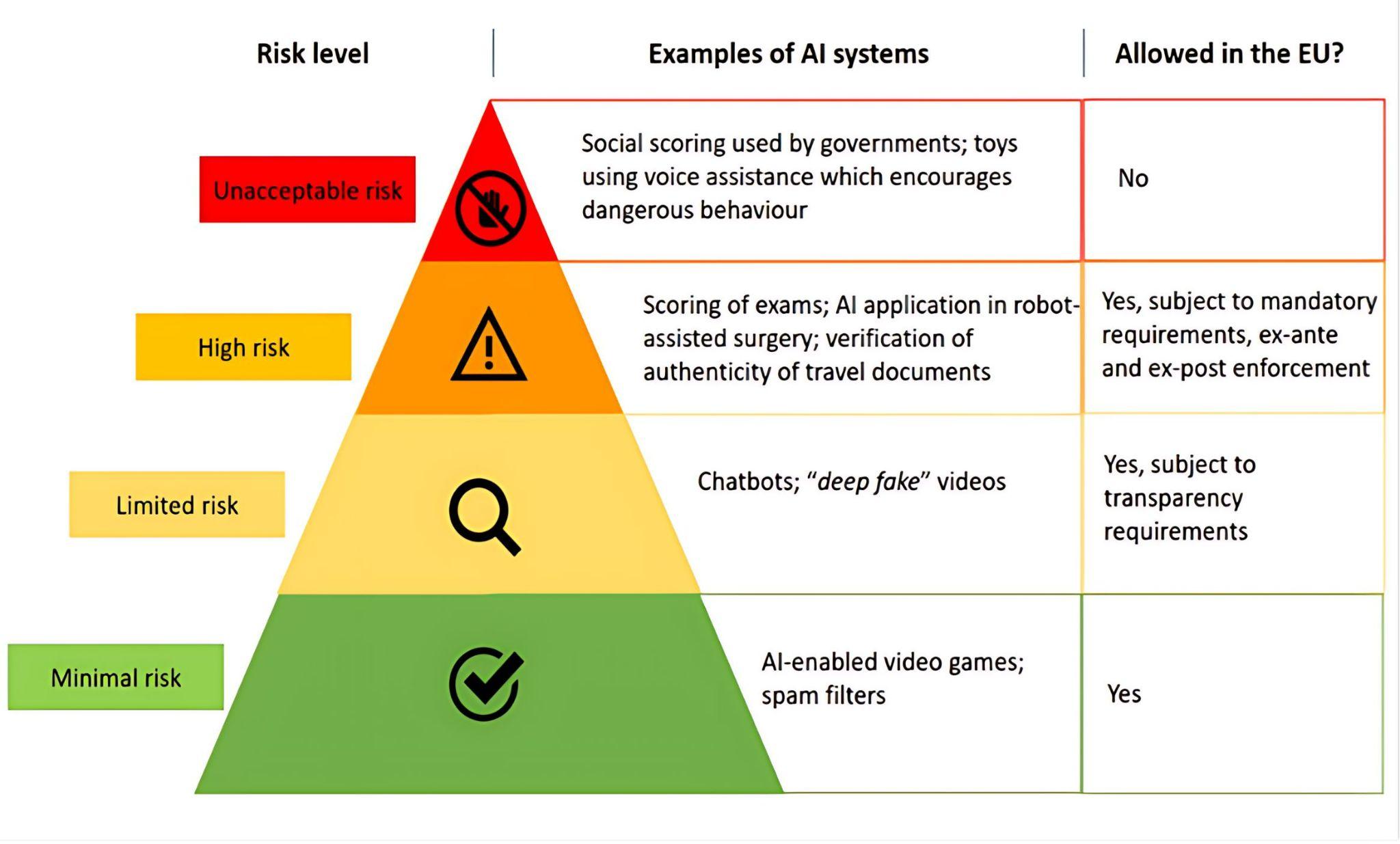
Enforcement is the other major difference between the EU and the US. The EU AI Acts’ risk model is premised upon ***prevention*** with general guidelines, specific penalties, and centralized regulation that prohibit activities unless explicitly permitted. In contrast, the current US risk model is ***permissive***: it promotes innovation through competition, encourages decentralized self-regulation, and relies upon an extensive network of existing laws and regulations against abusive, illegal, and negligent practices. These networks of existing laws range over a spectrum from specific consumer protection laws to general contract and tort enforcement to evolving intellectual property laws. This permissive approach follows the American tradition of tech sector self-regulation with notable success in sectors like online advertising (DAA, NAI), cybersecurity (NIST, CISA), biotechnology (IGSC, IASB), nanotechnology (ISO, NanoRisk), and cloud computing (CSA).

### **3. The European Union**

#### **3.1. Overview**

(2.1.Roles and Responsibilities)

(perhaps add a simple diagram before introducing the complex diagram to help orientate the reader to the big picture first - some variation of the canonical 4-layer risk pyramid like this one)



(source: <https://www.aipolicyconsulting.com/the-eu-s-new-rules-on-ai>)

#### **3.2. Laws and Regulation**

(General sections on how EU regulation works and how the EU AI Act was created within this framework)

#### **3.3. EU AI Act: Roles and Risks**

(Copy/Reorganize Text like Innovation, etc.)

(Complex EU AI Act Flowchart with walk-through explanation)

### **4. China**

#### **4.1. Overview**

China’s approach to AI governance and regulation is a hybrid between the centralized, top-down approach of the EU and the decentralized, free-market, competing interests model in the US. Like the EU, China emphasizes safety, individual protections, and social harmony through top-down guidance, regulation, and enforcement (Zhang 2022). Like the US, China also emphasizes bottom-up innovation and economic development with a mix of decentralized provincial control and very competitive local markets. Each approach has it’s advantages. The EU AI Act benefits from a coherent, universal risk-based approach, but the abstract and ambiguous language belies the hard work of grappling with real-world details in applying these general rules to disparate complex situations. Conversely, a fragmented, sector-specific approach like the US EO #14110 lacks coherent high-level simplicity but benefits from experienced domain expert regulators effectively translating stated goals into more clear, immediate, and effective enforcement. China seeks to benefit from the coherence of the EU AI Act with the practicality and benefits of the US approach to promoting innovation and economic competitiveness.

#### **4.2 Laws and Regulations**

China has advanced some of the first AI laws and regulations at the national level, which are summarized in Table X. Unlike the horizontal risk-based approach of the EU, China has favored the sector-specific US approach of laws tailored to specific use-cases. These specific use-cases range from personal privacy (November 2021) to recommendation algorithms (March 2022) to generative AI (January & August 2023). Despite appearances of centralized CCP control, these regulations are the product of an iterative process involving diverse stakeholders that include mid-level bureaucrats, academics, corporations, startups, and think tanks (Sheehan 2024). The central government relies upon a pipeline of these experts to formulate, clarify, and interpret the details, while they mainly concern themselves with ensuring goals and outcomes are aligned with Chinese and socialist ideology (Zhang 2022). Both China’s State Council and the Chinese Academy of Social Sciences have announced intentions of working towards a more holistic National AI law although the outcome is uncertain (Webster 2023).

| **Date** | **Title** | **Issuing Body** | **Description** |
| --- | --- | --- | --- |
| June 1, 2017 | Cybersecurity Law | National People's Congress | Establishes legal frameworks for cybersecurity, including data protection and network security, which indirectly impact AI development and deployment. |
| September 1, 2021 | Data Security Law | National People's Congress | Provides regulations on data processing and security, affecting AI systems that process large amounts of data. |
| November 1, 2021 | Personal Information Protection Law (PIPL) | National People's Congress | China's comprehensive data privacy law that governs the collection, storage, use, and transfer of personal information, impacting AI systems that handle personal data. |
| March 1, 2022 | Algorithm Recommendation Regulation | Cyberspace Administration of China (CAC) | Regulates algorithms used for content recommendations, requiring transparency and fairness, and prohibiting practices that disrupt public order. |
| January 10, 2023 | Provisions on Management of Deep Synthesis in Internet Information Service (Deep Synthesis Regulation) | CAC | Governs generative AI technologies, focusing on the authenticity and traceability of AI-generated content to prevent misinformation. |
| August 15, 2023 | Interim Measures for the Management of Generative Artificial Intelligence Services (Generative AI Measures) | CAC and six other authorities | Targets generative AI services, imposing obligations on service providers to ensure legality, fairness, and cybersecurity of AI-generated content. |
| October 1, 2022 (Shanghai) November 1, 2022 (Shenzhen) | AI Industry Promotion Regulations in Shanghai and Shenzhen | Shanghai and Shenzhen Municipal Governments | Local regulations to promote AI development, including ethical oversight and support for innovation within the AI industry. |
| Expected in 2024/2025 | Draft Artificial Intelligence Law (AI Law) | State Council (drafting stage) | A comprehensive national AI law is being drafted, aiming to provide an overarching legal framework for AI governance in China. |

**Table X** Chinese AI Laws and Regulations

#### **4.3 Registration and Compliance**

On paper China has perhaps the most onerous AI regulation requirements of the three regions considered in this paper. Table.Y lists the three major steps for deploying advanced AI models like Baidu’s ERNIE LLM to be in compliance with regulatory laws. These include model registration, rules for data management, and provisions for ongoing monitoring for compliance. The registration process alone illustrates how strict central regulation can slow down innovation and economic growth. As of March 2024, only 546 AI models have been registered, and just seventy are Large Language Models (China Money Network 2024). This number is in stark contrast to the countless commercial models, variants, and over 500,000 open-source LLMs on Huggingface.co (Huggingface.co 2024) which is banned in China (ChinaTalk 2023).

| **Model Registration** | |
| --- | --- |
| Approval Process | AI Models, especially Generative and LLM, must undergo through review for compliance with regulatory standards by the CAC and other bodies |
| Public Use/Licensing | After approval, all models must be registered for public use |
| Sector-Specific Approvals | Approval by additional sector-specific regulatory bodies may be required (e.g. healthcare, finance, security) |
| **Data Management** | |
| Source and Legitimacy | All training data must come from legitimate and lawful sources and be accurately labeled and documented to ensure traceability and accountability |
| Privacy Protection | All companies must comply with China’s privacy laws (e.g. PIPL) and implement robust measures to protect personal data and prevent misuse |
| Content Verification and Censorship | Providers must ensure training data does not contain prohibited data like politically sensitive or controversial content that could disrupt public order or national security (often requires moderation tools and manual checks) |
| Foreign-Language Content | Training data must include foreign language content to enhance global competitiveness |
| **Compliance Obligations** | |
| Security Assessment | Before launch, mandatory comprehensive security assessments to identify potential risks and vulnerabilities |
| Algorithm Registration | Registration of all algorithms including details on their design, functionality, and impacts on users and society |
| Ethical/Legal Compliance | Audit for compliance with ethical and legal standards, especially in avoiding inaccuracies, discrimination, and the perpetuation of biases against individual or groups |
| Ongoing Monitoring and Reporting | Continuous monitoring for system errors or deviations from approved conditions of use to allow for timely corrections |

**Table Y** AI Model Compliance Steps in China

Despite such rigorous guidelines, enforcement in China is relative lax with startups as well as small to mid sized enterprises (SMEs) flying under the radar as long as they do not have a large public presence (Zhang 2022). This allows for the promotion of innovation, economic growth, and international competitiveness (Yang 2024). In 2015, China announced a national strategic plan and industrial policy called “Made In China 2025” (MIC2025) integrated with their 13th (2016-2020) and 14th (2021-2025) Five Year Plan (State Council PRC 2015). MIC2025 directs strong government support for innovation and high-end manufacturing to help make China a global leader in cutting-edge technologies like AI by 2025 (CRS 2019). Part of this plan calls for supporting 10,000 “Little Giants” - small and mid-sized enterprises (SME) recognized as a key source of innovation (Global Times 2021). Although large “National Champions” like Baidu, Tencent, and Alibaba are expected to fully comply with AI regulations because of their dominant influence, the little giants are informally afforded leeway in order to avoid heavy regulatory burdens that could stifle innovation (Zhang 2024).

China’s hybrid system of AI regulation and selective enforcement attempts to combine the strengths of both the EU and the US approaches. While regulatory guidance is generally light, top-level enforcement usually comes into play when destabilizing patterns arise. This reactive enforcement can cause transitory market disruptions and lead to strict and sometimes surprisingly punitive measures to reign in excesses and outcomes at odds with CCP values like “common prosperity” (Caixin Global 2021) (Wu 2022). This pattern of regulatory crackdown is visible in other sectors, from real estate (Bloomberg 2021) to education (Intresse 2024). Harsh government penalties by government regulators between 2020-2022 were levied to try to control excessive inequality and check the rise of powerful tech (Alibaba) or financial (Ant Group) corporations that could challenge government authority (Chen 2023). Although deflating the real estate bubble significantly reduced household wealth tied to property speculation, the IMF shows China leads the world’s largest economies with a 5.2% GDP growth due to automation efficiencies, continuing up the tech value chain, and trade (IMF 2024). Some of this success is attributed to China’s strategic industrial policy including a flexible regulatory framework. This has also led to China’s dominance in the majority of the sixty-four critical technologies tracked by the Australian Strategic Policy Institute including renewable energy, telecommunications, and EVs (Gaida 2023).

### **CONCLUSION**

The EU, US, and China are each evolving distinct regulatory systems that vary in approach and emphasis. The EU AI Act proposes a coherent, universal risk-based regulatory framework with strict and well-defined penalties. It is criticized, however, for stifling innovation, for ambiguous language, and for expected challenges in implementation details across heterogeneous use cases. The Biden Whitehouse Executive Order on “Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence” is the most organized plan within the US on AI regulation that delegates over 100 specific tasks to over 50 federal agencies to build out AI expertise and oversight according to specific domain expertise. The decentralized US approach also involves smaller regulatory initiatives by the US Congress, individual States, and even cities. This reflects the US market-driven approach of competing stakeholders. On the other hand, this approach has come under criticism for relying too heavily on self-regulation and for being susceptible to flaws like regulatory capture. The Chinese approach to AI regulation synthesizes the US approach of use-case specific laws with a general guidelines that have been translated into centralized and comprehensive registration, testing, and monitoring framework. At the same time, innovation and economic growth is directly and indirectly supported by initiatives like investment in thousands of ‘little dragons’ alongside relatively lax enforcement for SMEs. This hybrid approach has led to a variety of surprising number of technological breakthroughs and economic success so far. Growing tensions and competition between the US and China are shifting Chinese AI regulation towards faster innovation and technological independence. Conversely, the US has steadily increased tariffs, export bans and sanctions on trade involving strategic technologies like AI, advanced chips, and semiconductor manufacturing equipment that may lead to pressure to curtail open source via more regulation.

**CONTRIBUTIONS**

* Christian Schroeder: The European Union
* Kathrine L. Elkins: The United States
* Jon Chun: China

Each author has approved the final version of the manuscript and agrees to be accountable for all aspects of the work in ensuring that questions related to the accuracy or integrity of any part of the work are appropriately investigated and resolved.

**Post NeurIPS 2+ papers to follow-up**

* Sec & RMF
* AI Reg, IndPol, TechGnd

### **REFERENCES**

Bloomberg News (2021, July 28). "In its latest crackdown, China intensifies focus on real estate". Aljazeera.com. Retrieved from https://www.aljazeera.com/economy/2021/7/28/in-its-latest-crackdown-china-intensifies-focus-on-real-estate (accessed May 2, 2024)

Office of Senator Richard Blumenthal. (2024, April 2). Blumenthal & Hawley Announce Bipartisan Framework on Artificial Intelligence Legislation. Retrieved from https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-and-hawley-announce-bipartisan-framework-on-artificial-intelligence-legislation (accessed May 2, 2024)

Caixin Global (2021, Oct 19). "Full Text: Xi Jinping's Speech on Boosting Common Prosperity". Retrieved from https://www.caixinglobal.com/2021-10-19/full-text-xi-jinpings-speech-on-boosting-common-prosperity-101788302.html (accessed May 2, 2024)

Chen, Lulu Yilun and Liu, Li. (2023, July 7). "China Ends Tech Crackdown With Fines on Tencent, Ant Group". Bloomberg.com. Retrieved from https://www.envoy.cirrus.bloomberg.com/news/articles/2023-07-07/china-ends-probe-of-jack-ma-backed-ant-with-984-million-fine?srnd=premium (accessed May 2, 2024)

ChinaTalk. (2023, Oct 19). "Hugging Face Blocked! 'Self-Castrating' China’s ML Development + Jordan at APEC". Retrieved from https://www.chinatalk.media/p/hugging-face-blocked-self-castrating (accessed May 2, 2024)

China Money Network. (2024, March 7). "Chinese tech giants dominate AI algorithms with a focus on industry-specific applications". Retrieved May 2, 2024, from https://www.chinamoneynetwork.com/2024/03/07/chinese-tech-giants-dominate-ai-algorithms-with-a-focus-on-industry-specific-applications (accessed May 2, 2024)

Congressional Research Service (CRS). (2019, April 12). "The Made in China 2025 Initiative: Economic Implications for the United States". Retrieved from https://crsreports.congress.gov/product/pdf/IF/IF10964/4 (accessed May 2, 2024)

Congressional Research Service (CRS). (2024). Highlights of the 2023 Executive Order on

Artificial Intelligence for Congress. Retrieved from https://crsreports.congress.gov/product/pdf/R/R47843/8 (accessed May 2, 2024)

European Parliament and Council of the European Union. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) [2016] OJ L 119/1. https://data.europa.eu/eli/reg/2016/679/oj

Gaida, Dr. Jamie, Leung, Dr. Jennifer Wong, Robin, Stephan, and Cave, Danielle (2023, Sep 22) ASPI’s Critical Technology Tracker - Sensors & Biotech updates. https://www.aspi.org.au/report/critical-technology-tracker. Australian Strategic Policy Institute. (accessed 19 Apr 2024)

Global Times. (2021, July 5). "China to develop 10,000 ‘little giants’ in push for advanced manufacturing" GlobalTimes.cn. Retrieved from https://www.globaltimes.cn/page/202107/1227877.shtml (accessed May 2, 2024)

Huggingface.co. (2024, May 2). Models. Retrieved from <https://huggingface.co/models> (accessed May 2, 2024)

International Monetary Fund (IMF). (2024, April 16). "World economic outlook: April 2024". IMF.org. Retrieved from https://meetings.imf.org/en/IMF/Home/Publications/WEO/Issues/2024/04/16/world-economic-outlook-april-2024 (accessed May 2, 2024)

Intresse, Giulia. (2024, Feb 23). "China’s New Draft Regulations for After-School Tutoring". China-Briefing.com. Retrieved from https://www.china-briefing.com/news/china-after-school-tutoring-new-draft-regulations-key-points/ (accessed May 2, 2024)

LegiScan (2024) California Senate Bill 1047: Safe and Secure Innovation for Frontier Artificial Intelligence Models Act, <https://legiscan.com/CA/text/SB1047/2023>. (accessed May 1, 2024)

Massoglia, Anna. (24 Jan 2024State and federal lobbying spending tops $46 billion after federal lobbying spending broke records in 2023. <https://www.opensecrets.org/news/2024/01/state-and-federal-lobbying-spending-tops-46-billion-after-federal-lobbying-spending-broke-records-in-2023>. OpenSecrets.com (accessed 1 May 2024)

National People's Congress of the People's Republic of China. (2016). Cybersecurity Law of the People's Republic of China (Adopted at the 24th Meeting of the Standing Committee of the Twelfth National People's Congress of the People's Republic of China on November 7, 2016). https://www.cac.gov.cn/2016-11/07/c\_1119867116.htm

Schumer, Senator Charles (21 Jun 2023). Sen. Chuck Schumer Launches SAFE Innovation in the AI Age at CSIS https://www.csis.org/analysis/sen-chuck-schumer-launches-safe-innovation-ai-age-csis Center fo Strategic and International Studies. (accessed May 1, 2024)

Sheehan, Matt. (2024, Feb 27). "Tracing the Roots of China’s AI Regulations." Carnegie Endowment for International Peace. Retrieved from https://carnegieendowment.org/2024/02/27/tracing-roots-of-china-s-ai-regulations-pub-91815 (accessed May 2, 2024)

\*\*\* (unused) Stallman, Richard. (1985). "The GNU Manifesto". Retrieved from https://www.gnu.org/gnu/manifesto.en.html. (accessed May 3rd, 2024)

The State Council of the People's Republic of China (State Council PRC). (2015). Made in China 2025. https://english.www.gov.cn/2016special/madeinchina2025/ (accessed May 2, 2024)

Webster, G., Zhou, J., Shi, M., Dorwart, H., Costigan, J., & Chen, Q. (2023, August 23). Forum: Analyzing an expert proposal for China's Artificial Intelligence Law. DigiChina, Stanford University. Retrieved from https://digichina.stanford.edu/work/forum-analyzing-an-expert-proposal-for-chinas-artificial-intelligence-law/ (accessed May 2, 2024)

The White House. (Oct 24, 2022) "Blueprint for an AI Bill of Rights." Statements and Releases <https://www.whitehouse.gov/ostp/ai-bill-of-rights/>. (accessed May 2, 2024)

The White House. (2023a, July 21) "FACT SHEET: Biden-⁠Harris Administration Secures Voluntary Commitments from Leading Artificial Intelligence Companies to Manage the Risks Posed by AI." Statements and Releases <https://www.whitehouse.gov/briefing-room/statements-releases/2023/07/21/fact-sheet-biden-harris-administration-secures-voluntary-commitments-from-leading-artificial-intelligence-companies-to-manage-the-risks-posed-by-ai/>. (accessed May 2, 2024)

The White House. (2023b, October 30). Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence. Retrieved from https://www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence/

The White House. (2024a, March 30). Administration Actions on AI. Retrieved from https://ai.gov/actions/

The White House. (2024b, April 29) "Biden-⁠Harris Administration Announces Key AI Actions 180 Days Following President Biden's Landmark Executive Order." Statements and Releases.<https://www.whitehouse.gov/briefing-room/statements-releases/2024/04/29/biden-harris-administration-announces-key-ai-actions-180-days-following-president-bidens-landmark-executive-order/>. (accessed May 2, 2024)

Wu, Guoguang. (2022). "China’s Common Prosperity Program: Causes, Challenges, and Implications". Retrieved from https://asiasociety.org/sites/default/files/2022-03/ASPI\_ChinaCommonProsp\_report\_fin.pdf (accessed May 2, 2024)

Yang, Zeyi. (2024, April 9). "Why the Chinese government is sparing AI from harsh regulations—for now". MIT Technology Review. https://www.technologyreview.com/2024/04/09/1091004/china-tech-regulation-harsh-zhang/ (accessed May 2, 2024)

Zeng, Hui, Jingyuan Xue, Meng Hao, Chen Sun, Bin Ning and Na Zhang. “Evaluating the Generation Capabilities of Large Chinese Language Models.” ArXiv abs/2308.04823 (2023): n. Pag.

Zhang, A. (2022). “High Wire: How China Regulates Big Tech and Governs Its Economy”. Oxford University Press.

Zhang, Angela Huyue. (2024, Mar 21). "How China Regulates Big Tech and Governs AI". Philip K.H. Wong Centre for Chinese Law. [Video]. YouTube. https://www.youtube.com/watch?v=NS1DGd2IXDs (accessed May 2, 2024)

### **Appendix A**

US federal entities involved in the Executive Order #14110 on AI Safety:

AIM-HEAD National Institutes of Health Artificial Intelligence/Machine Learning Consortium to Advance Health Equity and Researcher Diversity

A consortium to advance health equity and researcher diversity in AI/ML.

APDP Assistant to the President for Domestic Policy

Advises the President on domestic policy issues.

APEA Assistant to the President for Economic Affairs

Advises the President on economic policy issues.

APNSA Assistant to the President for National Security Affairs (a.k.a. the National Security Advisor)

Advises the President on national security and foreign policy issues.

CDOC Chief Data Office Council

A council that promotes data management and use within the federal government.

CEA Council of Economic Advisors

Advises the President on economic policy.

CEQ Council on Environmental Quality

Advises the President on environmental policy issues.

CISA Cybersecurity and Infrastructure Security Agency

Leads the national effort to protect and enhance the resilience of US cyber infrastructure.

DCOSP The President's Deputy Chief of Staff for Policy

Assists the President's Chief of Staff in managing the White House policy staff.

DGPC Assistant to the President and Director of the Gender Policy Council

Advises the President on gender policy issues.

DHS Department of Homeland Security

Responsible for protecting the US from threats and ensuring public safety.

DNI Director of National Intelligence (Office of the)

Oversees and directs the implementation of the National Intelligence Program.

DOC Department of Commerce

Promotes job creation, economic growth, and sustainable development in the US.

DOD Department of Defense

Responsible for national defense and military matters.

DOE Department of Energy

Ensures US energy security and promotes scientific and technological innovation.

DOJ Department of Justice

Enforces federal law and administers justice within the US.

DOL Department of Labor

Fosters and promotes the welfare of US workers, job seekers, and retirees.

DOS Department of State

Leads US foreign policy and diplomatic efforts.

DOT Department of Transportation

Oversees the nation's transportation systems and infrastructure.

ED Department of Education

Establishes policy for and administers federal aid to education.

FACA Federal Advisory Committee Act

A law that governs the operation of federal advisory committees.

FARC Federal Acquisition Regulatory Council

Assists in the direction and coordination of government-wide procurement policy.

FedRAMP Federal Risk and Authorization Management Program

A government-wide program that provides a standardized approach to cloud security.

FERC Federal Energy Regulatory Commission

Regulates the interstate transmission of electricity, natural gas, and oil.

FPC Federal Privacy Council

An interagency council that coordinates government-wide privacy initiatives.

GSA General Services Administration

Manages federal property and supports the basic functioning of federal agencies.

HHS Department of Health and Human Services

Protects the health of Americans and provides essential human services.

HUD Department of Housing and Urban Development

Supports community development and homeownership.

ISCP Interagency Council on Statistical Policy

Coordinates statistical work across federal agencies.

IRA Independent Regulatory Agencies

Agencies that operate independently of the executive branch.

NASA National Aeronautics and Space Administration

Responsible for the civilian space program and aeronautics research.

NCD National Cyber Director

Leads the development and implementation of national cyber policy and strategy.

NIFA National Institute of Food and Agriculture

Provides leadership and funding for agricultural research and extension programs.

NIST National Institute of Standards and Technology

Promotes innovation and industrial competitiveness through standards and technology.

NSF National Science Foundation

Supports fundamental research and education in science and engineering.

NTIA National Telecommunications and Information Administration

Advises the President on telecommunications and information policy issues.

OMB Office of Management and Budget

Oversees the administration's budget development and execution.

OPPRP Office of Pandemic Preparedness and Response Policy in the White House

Coordinates the federal government's pandemic preparedness and response efforts.

OPM Office of Personnel Management

Manages the civil service of the federal government.

OSTP Office of Science and Technology Policy

Advises the President on the effects of science and technology on domestic and international affairs.

PCAST President's Council of Advisors on Science and Technology

Advises the President on science, technology, and innovation policy.

SRMA Sector Risk Management Agency

Agencies responsible for managing risks to critical infrastructure sectors.

Treasury Department of the Treasury

Manages federal finances and collects taxes.

USAID United States Agency for International Development

Administers civilian foreign aid and development assistance.

USDA Department of Agriculture

Develops and executes federal laws related to farming, forestry, rural development, and food.

USDC United States Digital Corps

A two-year fellowship that recruits early-career technologists to serve in the federal government.

USDS United States Digital Service

Works across the federal government to modernize digital services.

USG NSS United States Government National Standards Strategy

A strategy for developing and using voluntary consensus standards in federal agencies.

USTPO United States Patent and Trademark Office

Grants patents and registers trademarks.

VA Department of Veterans Affairs

Provides healthcare and benefits to military veterans.