Comparative Analysis of AI Regulation: A Global Policy Perspective from the EU, US and China

Christian Schroeder de Witt[1]
Katherine Elkins[2]
Jon Chun[2]

[1]Oxford
[2]Kenyon College

August 2024

1 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. Together they comprise approaches in AI innovation and 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. This paper presents these differing frameworks embed divergent judgments on the balance between safety versus innovation and cooperation versus competition. These emerging regulatory AI frameworks reflect differing stances in regards to trust in centralized authority versus trust in a decentralized free market of self-interested stakeholders.

2 Introduction

On 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, 2023. The Biden administration published its Blueprint for an AI Bill of Rights in October 2023, 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 2024, was now being actively worked out.

Underlying these varied 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.

3 AI Governance

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, regional competition, and economic development at the local levels like in 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 penalties [1, 2].

4 United States

4.1 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 [3]. This act moved beyond the voluntary commitments secured in July 2023 [4] and the AI Bill of Rights. 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 [3]. 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.

On August 28, 2024 the California Assembly passed SB 1047, the Safe and Secure Innovation for Frontier AI Models Act. Unlike the federal Presidental Executive Order, this state law is focused on creating a regulatory framework around registering and continual auditing of models that could present a danger to public safety. This AI regulation targets models with substantial investment in training and fine-tuning above given thresholds of $100M and $10M respectively.

4.2 Laws and Regulations

AI regulation in the US 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 [5], promoting fair markets [6], and safeguarding the environment [7] (see NSF, SEC and EPA mission statements and goals). 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. US States and municipalities can also add regulations in areas they feel federal regulations are inadequate or missing.

This approach is in keeping with historical norms. The philosophical distrust of centralized power is reflected in the very design of the American system of checks and balances between branches of government. A 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 a $46 billion state and federal lobby industry [8]. For these reasons, commercial applications of technology within the US have traditionally been regulated through various mechanisms including legislative action, executive orders, agency rulemaking, industry self-regulation, international agreements, and private self-regulation.

To remain competitive in rapidly changing world markets, US tech companies often pursue self-regulation as a strategy for tackling privacy, digital advertising, content moderation, and cybersecurity [9, 10]. We see a similar approach taken in the Biden-Harris approach to securing voluntary commitments by leading AI companies to manage the risks posed by AI [3]. Furthermore, international agreements or regulations are sometimes adopted by US companies to do business abroad as is the case for EU's GDPR [11] and China's Cyberse-

curity Law [12]. The regulatory process often combines these approaches, with laws providing the foundation for agency regulations involving public input and expert consultation as technologies and circumstances evolve.

The rapid pace of AI innovation and the immense potential impact of A, coupled with the lack of technical expertise in government, has reversed the normal sequence for enacting regulation that begins with the U.S. Congress. 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 [3]. Although somewhat exceptional for the US process of lawmaking, White House Presidential executive orders more closely match the top-down, centralized organization of the European Commission in Brussels and the CCP in Beijing.

In spite of this similarity to the E.U. and China, aspects of the order nonetheless reflect the distinct US approach that can be characterized as "bottom-up" and distributed rather than "top-down" and centralized. In contrast to the more centralized, top-down approach to AI regulation prioritizing safety (EU) and social stability (China), the United States takes a more distributed, multi-stakeholder approach to AI regulation that mirrors its earlier approaches to regulating new technologies.

While universal directives on AI are provided by 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 and agencies and even states [13]. EO #14110 organizes this distributed regulatory system with specific objectives and deadlines delegated to various federal agencies directly from the executive branch.

Meanwhile, the US legislative branch is considering dozens of individual bills [14]. Two notable, ambitious, and more restrictive plans have been introduced by Senator Schumer in the form of his SAFE initiative [2] and the Blumenthal-Hawley Framework [15]. Thune's 2023 AI Research, Innovation and Accountability Act would create enforceable accountability and transparency for high-risk systems. The REAL Political Advertisements Act [16] aims to limit the use of Generative AI in campaigns, The Stop Spying Bosses Act [17] aims to limit the use of AI by employers to surveil employees, and the No FAKES Act [18] aims to protect visual and voice likenesses of individuals. At this time, however, none have been passed. Meanwhile, individual US states and municipalities have passed laws and are debating more extensive regulation regarding AI [19].In 2023 more than 40 bills were proposed, and Texas and Connecticut adopted statutes focused on preventing discrimination [20]. In the 2024 legislative session, at least forty states, Puerto Rico, The Virgin Islands and Washington D.C. have introduced AI bills and six states, Puerto Rico, the Virgin Islands have adopted resolutions or passed legislation [21]. Given the general supremacy of federal laws and regulations in the US [22]. and in order 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.

4.3 White House Executive Order 14110

Since 2016 and over three different Presidential administrations, a number of executive orders related to AI have been issued. The Biden White House's October 2023 "Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" is the most comprehensive to date [3]. It directs over fifty federal agencies to take over one hundred specific actions addressing eight core policy areas listed in Table 1 below including: safety and security, innovation and competition, worker support, bias and civil rights, consumer protection, privacy, federal use of AI, and international leadership [23]. The eight policy areas are ranked by the aggregate number of requirements and federal entities assigned to each area. These arguably provide a loose guidance on the relevance of each policy area from the most relevant (federal use, safety/security, and innovation/competition) to the least (worker support). EO #14110 implements many guidelines in the 2022 AI Bill of Rights to ensure the responsible design and use of artificial intelligence with regards to civil rights and privacy in areas such as hiring, healthcare, and surveillance [24].

EO #14110 addresses many of the core concerns highlighted in the EU AI Act. It does so, however, with several key differences [25]. While the EU AI Act establishes a new regulatory agency, the EU AI Office, that coordinates with member states, industry and civil society, the current US strategy relies upon augmenting the extensive network of existing US federal agencies with pre-existing specialized domain expertise. 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 a new centralized regulatory framework.

Because the US approach involves over fifty federal agencies, it is also much more extensive in implementation details than the EU. It directly addresses broader issues like unemployment, education, research, and consumer protection. Finally, and again in contrast to the EU AI Act, this US strategy is arguably more immediately actionable given the over one hundred specific objectives. Many deadlines are 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. As of this writing, the White House 180-day deadlines had been met [26].

Enforcement is another major area of difference between the EU and the US. The EU AI Acts' risk model is premised upon prevention. General guidelines, specific penalties, and centralized regulation 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 wide spectrum, extending from specific consumer protection laws to evolving intellectual property laws [27]. This permissive approach follows the American tradition of tech sector self-regulation with its notable success in sectors like online advertising (DAA, NAI), cybersecurity (NIST, CISA), biotechnol-

Relevance	Policy Area	Requirements/Entities	Federal Entities *
HIGH	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+
MEDIUM	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
LOW	Worker support	4 requirements 2 entities	CEA, DOL

Figure 1: Executive Order #14110 on the Safe, Secure, and Trustworth Development and Use of AI (* see Appendix A agency acronyms)

ogy (IGSC, IASB), nanotechnology (ISO, NanoRisk), and in cloud computing (CSA).

Within this permissive structure, and in response to the White House EO 14110, the National Institute of Standards and Technology [28] established the US AI Safety Institute in January of 2024. Housed within the larger Department of Commerce, NIST was originally established to facilitate U.S. industrial competitiveness. The US AI Safety Institute has members from academia, industry, and nonprofits. This partnership mirrors the kind of decentralized and voluntary approach discussed earlier. The US AI Safety Institute's initial task forces focus on safety, evaluation, measurement, and risk management. Their work follows upon the initial Risk Management Framework published in April 2024 [29]. On July 12 2024 representatives from the US AI Safety Institute and the European AI Office met in Washington, D.C. and announced plans for further cooperation and collaboration [30].

4.4 California SB 1047

California Senate Bill 1047 (SB 1047: Safe and Secure Innovation for Frontier AI Models Act) introduced in February 2024 by Senator Scott Wiener, attempts to minimize potential societal impacts of AI in the face of rapid progress [1]. This bill emerged in response to growing concerns about the the unique threats powerful AI systems could present [31].

SB 1047 aims to establish a comprehensive AI regulatory framework in Cali-

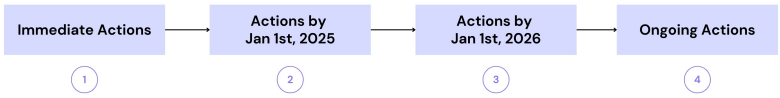

Figure 2: Action Timeline for SB 1047

fornia focused on the computational resources used to train and fine-tune models [32]. The bill has garnered support from a diverse coalition of stakeholders, including AI ethics researchers, civil rights organizations, and some technology companies advocating for responsible AI development [33, 34, 35]. However, it has also faced opposition from certain industry groups, politicians, and open-source adovocate that argue overly stringent regulations could stifle innovation, favor a handful of tech giants, and put California at a competitive disadvantage [36, 37, 38, 39].

Ongoing debates continue around the bill's potential impact on AI research and development, the feasibility of implementing some of its requirements, and the balance between fostering innovation and implementing safeguards [40, 41]. One of the most controversial aspects of SB 1047 is its requirement for developers to implement a full shutdown capability for covered AI models [42]. This raises concerns over potential disruptions to critical infrastructure and services that may rely on these systems, surfacing complex interdependencies and deep integration of AI with various sectors of the economy and society [1].

Since its introduction, SB 1047 has undergone several revisions in response to feedback from various stakeholders. Notable changes include refining the definition of "covered models" to more precisely target high-impact AI systems, clarifying the scope of the required safety and security protocols, and adjusting the timeline for compliance to allow companies more time to adapt to the new regulations [1]. These modifications demonstrate the iterative nature of the legislative process, particularly when dealing with rapidly evolving technologies like AI. As other jurisdictions, both within the United States and internationally, grapple with similar issues, the outcome of California's legislative efforts may have far-reaching implications for the future of AI regulation and development [40].

Unlike the EU AI Act, which adopts a comprehensive, risk-based approach to AI regulation across various sectors and applications, SB 1047 appears to focus more narrowly on high-impact AI systems, particularly those trained using substantial computational resources [43, 44]. This targeted approach may reflect a philosophy that prioritizes regulating the most powerful and potentially influential AI models, which could have far-reaching societal impacts.

The EU AI Act is characterized by its broad scope, clear enforcement mechanisms, and significant penalties for non-compliance [45]. For instance, the act proposes expanding obligations for organizations operating in the AI sector [46]. In contrast, the U.S. approach to AI regulation, which may influence SB 1047, typically involves adapting existing laws and regulatory frameworks to address

AI-specific challenges.

While the EU AI Act offers a degree of flexibility in implementation, allowing for tailored requirements for specific high-risk AI applications [47], it's unclear whether SB 1047 adopts a similar approach. The California bill's focus on computational resources used in AI model training suggests a unique regulatory philosophy that considers the scale and potential impact of AI systems as a key factor in determining regulatory requirements.

As shown in Figure 2 SB 1047's timeline for implementation and compliance is structured around specific milestones: immediate actions, actions required by January 1, 2026, actions required by January 1, 2027, and ongoing actions [48]. While detailed information about the specific requirements associated with each timeframe is not available, this phased approach suggests a recognition of the need for a gradual implementation process, allowing stakeholders time to adapt to new regulatory requirements.

4.4.1 Immediate Actions

Figure 3 outlines a series of immediate actions that developers of covered AI models must undertake if the SB 1047 is signed into law. These actions are designed to establish a framework for the responsible development, risk management, and public safety around the deployment of high-impact AI systems.

At the core of SB 1047's immediate requirements is the establishment of administrative, technical, and physical measures to prevent unauthorized access and misuse of covered models, with a particular focus on defending against advanced persistent threats and sophisticated actors. However, the bill's specific cybersecurity requirements are not explicitly detailed in the available sources.

Another key immediate action is the development of a safety and security protocol. This written document outlines procedures for managing risks throughout the model's lifecycle, including testing procedures to assess potential harm. However, the exact details of this protocol are not provided in the available sources.

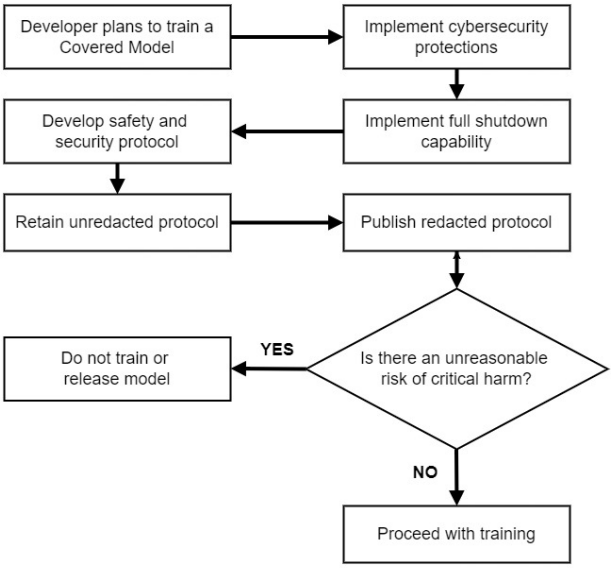

Figure 3: Immediate actions required according to CA SB 1047

4.4.2 Actions by January 2026

SB 1047 outlines a series of actions that developers of covered AI models must undertake by January 1, 2026, as illustrated in Figure 4. These actions are designed to enhance transparency, accountability, and safety in the development and deployment of high-impact AI systems.

A key requirement is the implementation of annual third-party audits. Starting January 1, 2026, developers must engage independent auditors to assess their compliance with the bill's requirements. These audits, conducted according to regulations issued by the Government Operations Agency, result in detailed reports evaluating internal controls and any instances of noncompliance. Developers are required to retain unredacted versions of these audit reports and provide access to the Attorney General upon request. In line with the bill's commitment to transparency, redacted versions of these reports must be published, with redactions limited to protecting sensitive information.

SB 1047 also mandates that developers submit annual compliance statements to the Attorney General. These statements, signed by the chief technology officer or a senior corporate officer, must include assessments of potential critical harms and verification of compliance with the bill's requirements. The bill also introduces a 72-hour reporting requirement for any AI safety incidents affecting covered models, emphasizing the importance of prompt disclosure and response to potential risks.

Furthermore, SB 1047 establishes a consortium within the Government Operations Agency tasked with developing a framework for "CalCompute," a public

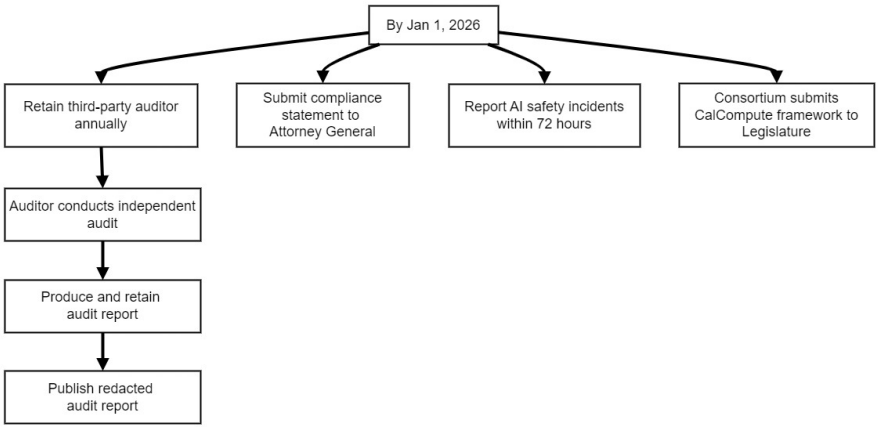

Figure 4: Actions required by Jan 1st, 2026 according to CA SB 1047

cloud computing cluster. This initiative, culminating in a report to be submitted to the Legislature by January 1, 2026, represents a forward-looking approach to creating public infrastructure for AI development and research. These actions, as outlined in Figure 4, collectively aim to create a more robust, transparent, and accountable ecosystem for the development and deployment of powerful AI systems.

4.4.3 Actions by January 2027

SB 1047 outlines a series of actions to be implemented by January 1, 2027, as illustrated in Figure 5. These actions are designed to establish a robust regulatory framework and governance structure for high-impact AI systems in California.

A key component of this phase is the establishment of the Board of Frontier Models within the Government Operations Agency. As shown in Figure 5, this board will consist of nine members with expertise in AI, safety, and related fields. The board's primary responsibility will be to approve regulations and guidance, ensuring that the regulatory framework remains informed by the latest developments in AI technology and safety considerations.

By January 1, 2027, and annually thereafter, the Government Operations Agency is mandated to issue a set of regulations, subject to approval by the Board of Frontier Models. These regulations serve three critical functions. First, they update the definition of "covered model," adjusting thresholds to reflect technological advancements and emerging risks. Second, they establish comprehensive auditing requirements, defining standards and best practices for the third-party audits introduced in the previous phase. Finally, the regulations provide guidance on preventing critical harm, offering recommendations to developers on risk mitigation strategies.

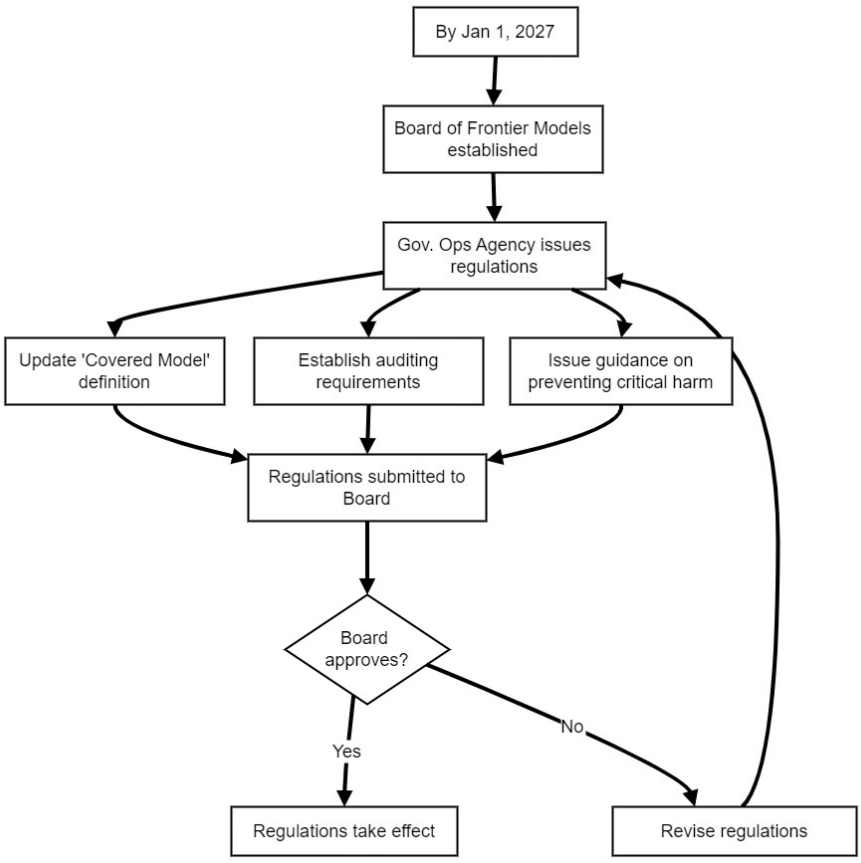

Figure 5: Actions required by Jan 1st, 2027 according to CA SB 1047

4.4.4 Ongoing Actions

SB 1047 outlines a comprehensive set of ongoing actions that developers and operators of high-impact AI systems must undertake to ensure continued compliance and safety, as illustrated in Figure 6. These actions are designed to create a dynamic and responsive regulatory environment that adapts to the rapidly evolving field of AI.

Developers are required to engage in annual re-evaluations and updates of their safety and security protocols. This process ensures that protocols remain current, accounting for changes in model capabilities and industry best practices. Complementing this internal review, the bill mandates the continuation of annual third-party audits, with the retention and publication of audit reports as specified.

Figure 6 also highlights the ongoing obligation for developers to report AI safety incidents within 72 hours of discovery, emphasizing the importance of prompt disclosure and response to potential risks. Additionally, the bill requires adherence to updated regulations issued by the Government Operations Agency, ensuring that developers remain compliant with the latest standards and definitions.

SB 1047 introduces important protections for whistleblowers, prohibiting retaliation against employees who report non-compliance or risks. This provision tries to foster a culture of openness and accountability within organizations developing high-impact AI systems. Furthermore, the bill outlines specific responsibilities for operators of computing clusters, including implementing policies to assess customers' use of compute resources, retaining records of customers using resources sufficient to train covered models, and maintaining the capability to enact full shutdowns if necessary.

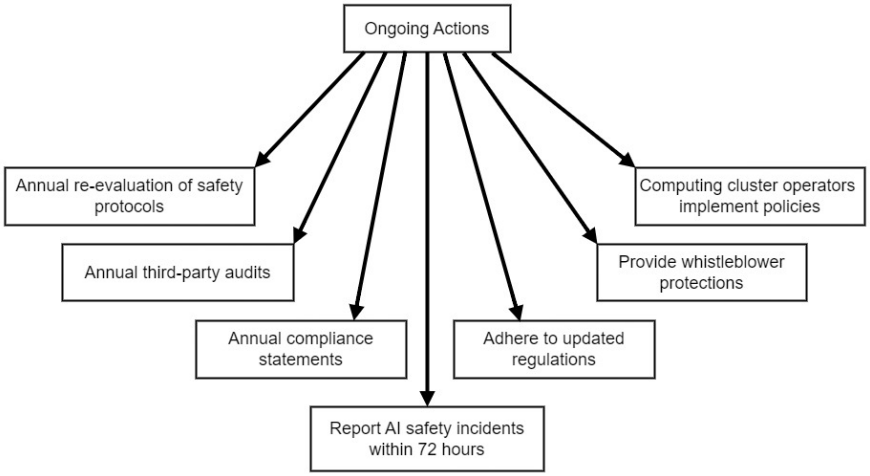

Figure 6: Ongoing Actions required according to CA SB 1047

4.4.5 Enforcement

SB 1047 establishes a robust enforcement mechanism to ensure compliance with its provisions. It is designed to provide the necessary authority and tools to address violations and protect the public interest in the responsible development and deployment of high-impact AI systems.

The Attorney General is granted significant authority in enforcing SB 1047 and is empowered to bring civil actions against entities that violate the bill's provisions. This authority extends to seeking a range of remedies, including civil penalties, injunctive relief to halt non-compliant activities, and damages where appropriate. Comprehensive enforcement power ensures that there are meaningful consequences for non-compliance, serving as a strong deterrent against potential violations.

The penalty structure is designed to be proportionate and impactful. Civil penalties are calculated based on the cost of compute used to train the model in question. This approach ensures that penalties are commensurate with the scale and potential impact of the AI system involved. Additionally, the bill provides for specific penalties for particular violations, such as misrepresentation by auditors, highlighting the importance of integrity in the audit process.

Protections and remedies are also established for whistleblowers. Employees who face retaliation for reporting non-compliance or risks are granted the right to seek injunctive relief. These protections are cumulative with other laws, ensuring comprehensive safeguards for individuals who come forward with concerns about potential violations or safety risks.

This enforcement framework creates a strong accountability mechanism. Combining substantial penalties, broad enforcement authority, and robust

whistleblower protections creates a regulatory environment to encourages compliance, transparency, and responsible AI practices.

5 The European Union

5.1 Overview

The 2024 EU AI Act is positioned as the world's first comprehensive AI law [49]. Just as prior European general purpose legislation, such as the 2016 General Data Protection Regulation (GDPR) [11], the EU AI Act represents complex joint efforts and interests across various EU bodies, including the European Commission, the European Parliament and the European Council, where the latter represents the Heads of State of all EU member countries. Influence on the Act's formation was also taken publicly by national government officials, such as France's premier Macron's overt lobbying for exemptions for open source AI providers such as Mistral [39], as well as, both publicly and covertly, by lobbying and industry groups, including Big Tech [50], and German pro open-source non-profit LAION [51].

Uniquely, the Act was first constructed within a product safety framework, but then blended with a fundamental rights agenda at the behest of the European Parliament and against pressure by the European Commission [52]. This approach resulted in a unique and novel blend of legislative frameworks, clearly setting the EU AI Act apart from prior legislation building on established frameworks such as the GDPR. As Dragos Tudorache, a member of the European Parliament from Romania and the chair of the Special Committee on Artificial Intelligence in a Digital Age, remarked: "Regulation isn't just rules, it's an opportunity to express our values [53]."

While constituting an innovative syncretism at heart, the Act does follow and respect earlier European generalist regulatory initiatives, such as the GDPR, and the 2012 Digital Markets Act [54, DMA]. In fact, the EU started examining the compatibility of the GDPR and AI as early as in 2020 [55]. Nevertheless, the release of ChatGPT in November 2022 and its rapid adoption by millions of consumers worldwide caught European policymakers off-guard and led to significant adjustments to the Act's handling of AI governance. On December 9th, 2023, the Act was provisionally agreed between the European Parliament and the European Council. During the 3-day round of negotiations, the Act's scope was tightened [56]. It was clarified that the Act does not apply outside of European law, does not infringe on the security competences of the member states or so-entrusted entities, nor any military or defense applications. Importantly, it was clarified that the Act would not apply to sole purposes of research and innovation, nor other non-professional use. Most importantly, the Act's traditional approach to AI systems risk classification was complemented by the notion of general-purpose AI systems (GPAI) [49, Article 3(63)], resulting in a parallel governance track for such AI systems. Despite open questions, the Act's ambition to distinguish between GPAI and non-GPAI systems, and GPAI

systems of *systemic risk*, is similarly unique among AI regulations globally.

5.2 The Geopolitics of the Act

Besides regulating the EU single market, the Act is widely regarded as a strategic effort by the European Commission to establish themselves as the leading AI rulemakers globally [57]. Just as after the adoption of the GDPR in 2016 [11], it is speculated that companies across the world will begin to prioritize compliance with European AI law out of economic necessity, not through coercion [58]. In the case of the GDPR, this form of "Brussels Effect" [59] was complemented by a "de jure" effect in which countries with a lack of their own regulatory capacity, such as many developing countries, incorporated EU laws instead. For example, the Philippinesincorporated the right to be forgotten into their Data Privacy Act of 2012 [60, 61]. In a similar way, it is speculated that the EU AI Act may similarly become the de-facto standard for AI governance in much of the Western and developing world [58].

One direct institutional consequence of the EU AI Act is the establishment of a novel authority under the helm of the European Commission, namely the EU AI Office. This new office will not only oversee AI regulation and AI systems' compliance, provide a central pool of AI expertise to the EU's member states, but also provides a "strategic, coherent, and effective European approach on AI at the international level" [62]. A specialist position, The Advisor for International Affairs, will represent the AI Office in "global conversations on convergence toward common approaches" [63]. The EU AI Office therefore is not only meant to consolidate the EU's approach to AI regulation within the European market, but will likely centrally support the EU's foreign policy ambitions in economic and trade negotiations.

5.3 Laws and Regulation

The Act is designed as an *adaptive legislation*, meaning that many details are intentionally left vague to permit later adaptation as technology changes. At its core lies a risk classification system that puts obligations mostly on the developers ("providers") of AI systems. Importantly, the Act not only applies to systems that are placed on the market or put into service in the EU, but also to AI systems whose output is used in the EU. The use of AI systems for national security, research, or recreational purposes, as well as, more generally, end-users of AI systems are excluded from regulation under the Act.

5.3.1 Systems and Models

The AI Act adopts the definition of *AI system* from the OECD's AI Principles, defining an AI system as *"a machine-based system that is designed to operate with varying levels of autonomy and that can, for explicit or implicit objectives, generate outputs such as predictions, recommendations, or decisions that influence physical or virtual environments"* [64]. *AI models*, conversely, are

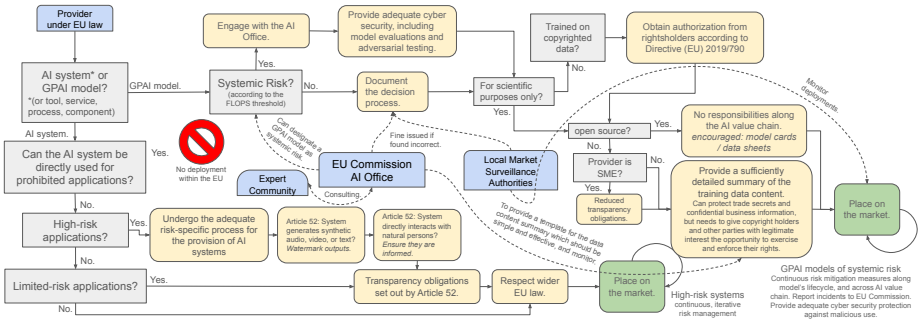

Figure 7: Decision tree for providers of (GP)AI systems and GPAI models on the way to the EU market.

mathematical algorithms or trained models that, in isolation, lack additional components such as a user interface or hardware integration that would allow them to be used as an AI system.

Among models, the Act further disambiguates between non-GPAI and *general-purpose AI (GPAI) models*, with the latter defined as *"an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market"* [49, Article 3(63)]. Where a GPAI model is integrated into an AI system, the system is referred to as a *GPAI system* provided that the system has the capability to serve a variety of purposes.

5.3.2 Roles

The Act fundamentally distinguishes between the roles of *provider*, *deployer*, *importer* and *distributor*. Providers are those *"placing on the market or putting into service AI systems or placing on the market general-purpose AI models in the Union"* [49, Article 2], irrespectively of their location. They have pre-market obligations including an initial risk assessment, risk-specific compliance, as well as risk-specific post-market obligations. Deployers are users of AI systems that are based on the EU and that don't fall within a small number of non-professional use cases. The Act furthermore distinguishes between AI models or systems provided or deployed from within the EU, and those from outside.

5.4 Risks

At the core of the EU AI Act lies a risk classification system for AI systems based on their possible "direct" use cases. In the case of GPAI systems, the

degree of "directness" is understood as the extent to which implemented safety measures can prevent risk-relevant use by deployers. If local market surveillance believe that a GPAI systems can be (or become) "directly" used for high-risk activities the EU AI Office will carry out the corresponding compliance procedures [49].

Prohibited use cases. Integrating fundamental human rights into the product safety framework, the Act defines a class of *prohibited AI practices*, such as placing on the market AI systems that can be used for certain forms of manipulation and exploitation, social scoring purposes, and certain biometric identification purposes. Furthermore, the deployment of AI systems that leave the user uninformed about their interaction with an AI system, emotion recognition systems or biometric categorisation systems, or AI systems producing deepfakes are all likewise prohibited [49, Article 5].

High-risk use. The class of *high risk* systems constitutes the majority of risk-related regulation [49, Article 6]. High-risk systems include a wide variety of systems as defined in [49, Annex I-III], including systems meant to serve as safety systems for other AI systems. According to [49, Article 28(2a)], providers of high risk systems are subject to compliance obligations, including the establishment of risk and quality management systems, data governance, human oversight, cybersecurity measures, postmarket monitoring, and maintenance of the required technical documentation. Owing to the Act's adaptive nature, it is expected that these obligations will be further detailed in later, sector-specific regulation.

Limited risk. Chatbots or AI systems that generate content or aid in decision-making without any critical safety aspects or significance are deemed of *limited risk*, although the Act only indirectly defines this class [49, Recital 32a]. These systems are merely subject to transparency obligations, including end-users of such systems must be informed that they are interacting with AI.

Minimal risk. AI systems that pose little to no risk to users' rights, health, or safety are left unregulated by the Act, although other obligations under EU law still apply. These systems are sometimes referred to as *minimal risk* although this term is not used in the Act.

Importantly, in the case of GPAI models, a special risk category is defined for the standalone model even before having been integrated into an AI system.

GPAI models of systemic risk. The Act imposes particular regulation on providers of general-purpose AI models of systemic risk [49, Article D], which it defines to be all models for which *"the cumulative amount of compute used for its training measured in floating point operations (FLOPs) is greater than* 10^{25}*"* [49]. The limit of 10^{25} was reportedly reached as a middle ground between 10^{24} and 10^{26} demanded by two opposing factions, the European Parliament,

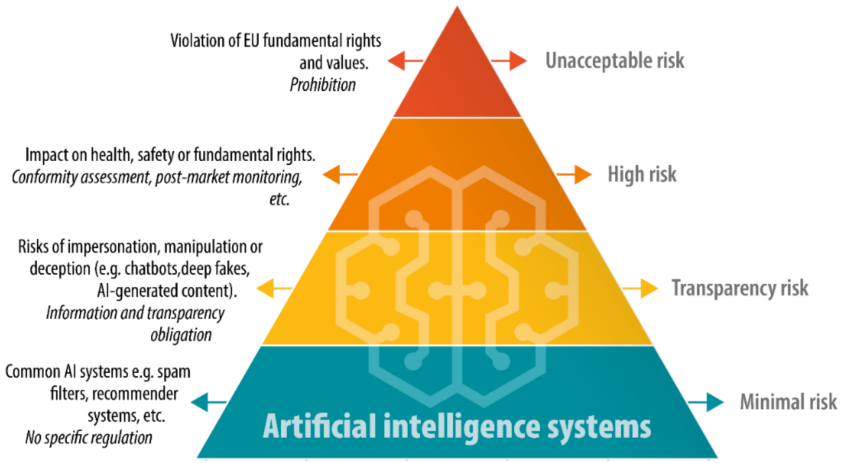

Figure 8: The risk pyramid for AI systems (taken from [65])

and the European Commission [49, Chapter II(8)][52]. Providers of GPAI need to register their model with the European Commission, and need to adhere to a wide-ranging catalogue of safety and security criteria. Owing to its adaptive nature, the Act purposefully leaves various technical criteria related to systemic risk classifications open for later adjustment to account for the unpredictability of technological progress.

5.5 Innovation and Open Source

The Act contains several measures intended to harness the economic and societal benefits of open-source AI software [66, 67]. The Act defines free and open-source AI components to cover "the software and data, including models and general-purpose AI models, tools, services or processes of an AI system" and explicitly states that provision of such models on open repositories should not seen as a form of monetization [49, Recital 103].

The EU Act contains wide-ranging exemptions for providers of certain AI systems provided under free and open source software licenses [49, Article 53-54]. To be exempt, the systems may not contain GPAI models that fall within the systemic risk category, or otherwise exhibit unacceptable behavior. The Act distinguishes the above from providers of pre-trained AI models that are made accessible to the public under a license that allows for the access, usage, modification, and distribution of the model, and whose parameters, including the weights, the information on the model architecture, and the information on model usage, are made publicly available. It is to be noted that the term open source model is not used explicitly and the degree of legal overlap with open source software is not immediately clear, and hence such models might be referred to rather as open models. Open models are not exempt from Article [49,

C(1)(c)-(d)], as well as [49, Article D] and [49, Article 28(2a)], the latter governing third-party obligations "along the AI value chain of providers, distributors, importers, deployers or other third parties" [55] for high-risk AI systems.

Under any circumstances, providers of open GPAI model providers are responsible for transparency obligations according to [49, Article C(1)(c)-(d)]. These transparency requirements include respecting existing Union copyright law [49, Article C(1)(c)] according to Article 4(3) of the Digital Single Market Directive (EU) 2019/790 [68], and the need to make a *"sufficiently detailed summary of the content used for training of the general-purpose AI model"* [49, Article C(1)(d)]. The consequences of these transparency requirements for open GPAI model providers have been examined in [69]. Importantly, Directive (EU) 2019/790 expands GDPR regulation to copyright owners who share content online, meaning that key GDPR rights, such as the right to opt out [11, GDPR Article 7] would require that copyright owners could ask for their data to be removed from open GPAI model training data.

As a further measure to stimulate innovation, member states can establish a regulatory sandbox, i.e. a controlled environment that facilitates the development, testing and validation of innovative AI systems (for a limited period of time) before they are put on the market [65].

6 China

6.1 Overview

China's approach to AI governance and regulation is a hybrid between the centralized, universal top-down approach of the EU and the decentralized, specialized free-market of competing interests in the US. Like the EU, China emphasizes safety, individual protections, and social harmony through top-down guidance, regulation, and enforcement [70]. Like the US, China also emphasizes bottom-up innovation and economic development through a mix of decentralized provincial control alongside very competitive local markets. This hybrid approach seeks to optimize the benefits from both the EU and US models. The EU AI Act takes 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 and highly situational cases. Conversely, a fragmented, sector-specific approach like the US EO #14110 lacks coherent high-level simplicity but benefits from experienced domain experts translating 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 that promotes innovation and economic competitiveness.

6.2 Laws and Regulations

China has advanced some of the first AI laws and regulations at the national level, which are summarized in Table 2. 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 data privacy (November 2021) to recommendation algorithms (March 2022) to generative AI (January & August 2023). Despite appearances of centralized government control, Chinese AI regulations are the product of an iterative process involving diverse stakeholders that include mid-level bureaucrats, academics, corporations, startups, and think tanks [71]. 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 [70]. 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 [72].

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.

Figure 9: Chinese AI Laws and Regulations

6.3 4.3 Registration

On paper, China has perhaps the most onerous AI regulation requirements of the three regions considered. Table 3 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 [73]. This number is in stark contrast to the countless commercial models, variants, and over 500,000 open-source LLMs on Huggingface.co [74], which is banned in China [75].

6.4 Compliance and Industrial Policy

In 2015, China announced a national strategic plan and industrial policy called "Made In China 2025" or MIC2025 integrated with their 13th (2016-2020) and 14th (2021-2025) Five Year Plan [76]. 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 [77]. Part of this plan calls for supporting 10,000 "Little Giants," the small and mid-sized enterprises (SME) recognized as a key source of innovation [78]. 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 [79].

What this means from a practical standpoint is that despite such rigorous guidelines, enforcement in China is relatively lax. Startups and SMEs fly under the radar as long as they do not have a large public presence [70]. This approach allows for the promotion of innovation, economic growth, and international competitiveness [80].

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" [81]. This pattern of regulatory crackdown is visible in other sectors from real estate[82] to education [83]. 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 [84]. 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 [85]. Some of this success is attributed to China's strategic industrial policy including a flexible regulatory framework.

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 aimplement 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

Figure 10: AI Model Compliance Steps in China

7 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 White House Executive Order on "Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence" is the most organized plan in the US that delegates over one hundred specific tasks to over fifty 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 general guidelines that have been translated into a 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 technological breakthroughs and economic success, but it risks criticism of capriciousness given that regulations are not uniformly applied. 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. These geopolitical tensions mean that the regulatory landscape will continue to evolve as countries re-evaluate their stance towards risk/innovation tradeoffs along with their desire to remain at the forefront of AI development.

8 Contributions

- Christian Schroeder de Witt: The European Union
- Katherine L. Elkins: The United States
- Jon Chun: The United States and China

Each author has reviewed each other's section and takes responsibility for the content of their own.

9 References

10 Appendix A

References

[1] LegiScan. California senate bill 1047: Safe and secure innovation for frontier artificial intelligence models act, 2024. Accessed May 1, 2024.

[2] Charles Schumer. Sen. chuck schumer launches safe innovation in the ai age at csis, June 2023. Accessed May 1, 2024.

[3] The White House. Executive order on the safe, secure, and trustworthy development and use of artificial intelligence, October 2023.

[4] The White House. Fact sheet: Biden-harris administration secures voluntary commitments from leading artificial intelligence companies to manage the risks posed by ai, July 2023. Accessed May 2, 2024.

[5] National Science Foundation. About, 2024. Accessed July 16, 2024.

[6] Security and Exchange Commission. About and mission, 2024. Accessed July 16, 2024.

[7] Environmental Protection Agency. About page, our mission and what we do, 2024. Accessed July 16, 2024.

[8] Anna Massoglia. State and federal lobbying spending tops $46 billion after federal lobbying spending broke records in 2023. *OpenSecrets.com*, January 2024. Accessed May 1, 2024.

[9] M. A. Cusumano, A. Gawer, and D. B. Yoffie. Social media companies should self-regulate. now. *Harvard Business Review*, January 2021.

[10] M. Minow and N. Minow. Social media companies should pursue serious self-supervision— soon: Response to professors douek and kadri. *Harvard Law Review*, June 2023.

[11] 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 (general data protection regulation), article 7, 2016. Accessed: 2024-09-08.

[12] National People's Congress of the People's Republic of China. Cybersecurity law of the people's republic of china, November 2016. Adopted at the 24th Meeting of the Standing Committee of the Twelfth National People's Congress of the People's Republic of China.

[13] Perkins and Coie. States begin to regulate ai in the absence of regulation, May 2024. Accessed July 16, 2024.

[14] GovTrack.us. Govtrack.us, 2024. Accessed 16 Sept. 2024.

[15] Office of Senator Richard Blumenthal. Blumenthal & hawley announce bipartisan framework on artificial intelligence legislation, April 2024. Accessed May 2, 2024.

[16] Amy Klobuchar. Real political advertisements act, 2023.

[17] Robert P. Casey. Stop spying bosses act, 2023.

[18] Chris Coons, Marsha Blackburn, Amy Klobuchar, and Thom Tillis. No fakes act, 2023.

[19] International Association of Privacy Professionals. Us state ai governance legislation tracker, 2024. Accessed 16 Sept. 2024.

[20] White and Case. Ai watch global regulatory tracker us, 2024.

[21] National Conference of State Legislatures. Ai 2024 legislation, June 2023. Accessed July 12, 2024.

[22] Justia US Law. The operation of the supremacy clause, 2024. Accessed July 16, 2024.

[23] The White House. Administration actions on ai, March 2024.

[24] The White House. Blueprint for an ai bill of rights, October 2022. Accessed May 2, 2024.

[25] Congressional Research Service. Highlights of the 2023 executive order on artificial intelligence for congress, 2024. Accessed May 2, 2024.

[26] The White House. Biden-harris administration announces key ai actions 180 days following president biden's landmark executive order, April 2024. Accessed May 2, 2024.

[27] D. Walters and H. J. Wiseman. Self-regulation in the cradle: The role of standards in emerging industries. *SSRN Electronic Journal*, 2022.

[28] NIST. About, 2024.

[29] NIST. Ai risk management framework, 2024.

[30] NIST. Ai safety institute and european ai office hold technical dialogue, July 2024. Accessed July 16, 2024.

[31] GDPR Local. California's senate bill 1047: Key takeaways on california's ai safety bill, 2024. Accessed: 2024-09-16.

[32] Stephen M. Anstey and Michael J. Breslin. Proposed california ai law sb 1047 – an overview for developers, 2024. Accessed: 2024-09-16.

[33] The Hill. Ai employees support california ai bill. *The Hill*, 2024.

[34] THE Journal. Anthropic offers cautious support for new california ai regulation legislation. *THE Journal*, August 2024.

[35] The Verge. California's sb-1047 ai industry regulation faces backlash. Accessed: 2024-09-16.

[36] Anjney Midha and Derrick Harris. California's senate bill 1047: What you need to know. *Andreessen Horowitz Blog*, 2023.

[37] Alden Abbott. Coalition letter opposing california sb 1047, June 2024.

[38] Neil Chilson and Kristian Stout. Coalition letter opposing california sb 1047, June 2024.

[39] Leila Abboud and Javier Espinoza. EU's new AI Act risks hampering innovation, warns Emmanuel Macron. *Financial Times*, December 2023.

[40] Foley and Lardner LLP. California dreamin': Sb 1047 and ai innovation. Accessed: 2024-09-16.

[41] Morgan Lewis. California's sb 1047 would impose new safety requirements for developers of large-scale ai models. Accessed: 2024-09-16.

[42] Neontri. California senate bill 1047. Accessed: 2024-09-16.

[43] Is california's sb-1047 the future of ai regulation?, 2024.

[44] A big win for the eu - how california's ai legislation compares to the eu ai act, 2024.

[45] Stephanie Renverseau. Ai act and sb-1047 - new guardians of ai. *Medium*, 2024.

[46] California sb 1047: Ai regulation bill, 2024.

[47] Sofia Gracias. Comparing eu ai act to proposed ai-related legislation in the us. *University of Chicago Business Law Review*, 2024.

[48] Deep dive into sb-1047, 2024.

[49] Regulation (eu) 2024/123 of the european parliament and of the council of 21 may 2024 laying down harmonised rules on artificial intelligence (artificial intelligence act), 2024. Accessed: 2024-09-08.

[50] Billy Perrigo. Exclusive: OpenAI Lobbied E.U. to Water Down AI Regulation, June 2023.

[51] A Call to Protect Open-Source AI in Europe | LAION.

[52] The Privacy Advisor Podcast: Inside the EU AI Act negotiations: A discussion with Laura Caroli.

[53] Josh Tyrangiel. Opinion | I found the smartest politician on AI. It's no one you'd expect. *Washington Post*, March 2024.

[54] European Parliament and Council of the European Union. Regulation (eu) 2022/1925 of the european parliament and of the council of 14 september 2022 on contestable and fair markets in the digital sector (digital markets act). `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R1925`, 2022. Official Journal of the European Union, L 265/1, 12 October 2022.

[55] Giovanni Sartor and Francesca Lagioia. The impact of the general data protection regulation (gdpr) on artificial intelligence. Study PE 641.530, European Parliamentary Research Service (EPRS), 2020. Scientific Foresight Unit (STOA), Panel for the Future of Science and Technology.

[56] Artificial intelligence act: Council and Parliament strike a deal on the first rules for AI in the world.

[57] The EU's new AI Act could have global impact | Chatham House – International Affairs Think Tank, March 2024.

[58] Marco Almada and Anca Radu. The Brussels Side-Effect: How the AI Act Can Reduce the Global Reach of EU Policy. *German Law Journal*, pages 1–18, February 2024.

[59] Anu Bradford. The Brussels Effect: How the European Union Rules the World. *Faculty Books*, March 2020.

[60] Republic of the Philippines. Republic act no. 10173: Data privacy act of 2012. `https://www.privacy.gov.ph/data-privacy-act/`, 2012. Enacted on August 15, 2012.

[61] Data Protected Philippines| Insights | Linklaters.

[62] European AI Office | Shaping Europe's digital future.

[63] Why work at the EU AI Office? | EU Artificial Intelligence Act.

[64] OECD. OECD Principles on AI, 2019. Accessed: 2024-09-08.

[65] Tambiama Madiega. Artificial intelligence act, 2024.

[66] Francisco Eiras, Aleksandar Petrov, Bertie Vidgen, Christian Schroeder de Witt, Fabio Pizzati, Katherine Elkins, Supratik Mukhopadhyay, Adel Bibi, Botos Csaba, Fabro Steibel, Fazl Barez, Genevieve Smith, Gianluca Guadagni, Jon Chun, Jordi Cabot, Joseph Marvin Imperial, Juan A. Nolazco-Flores, Lori Landay, Matthew Jackson, Paul Röttger, Philip H. S. Torr, Trevor Darrell, Yong Suk Lee, and Jakob Foerster. Near to Mid-term Risks and Opportunities of Open-Source Generative AI, May 2024. arXiv:2404.17047 [cs].

[67] Francisco Eiras, Aleksandar Petrov, Bertie Vidgen, Christian Schroeder, Fabio Pizzati, Katherine Elkins, Supratik Mukhopadhyay, Adel Bibi, Aaron Purewal, Csaba Botos, Fabro Steibel, Fazel Keshtkar, Fazl Barez, Genevieve Smith, Gianluca Guadagni, Jon Chun, Jordi Cabot, Joseph Imperial, Juan Arturo Nolazco, Lori Landay, Matthew Jackson, Phillip H. S. Torr, Trevor Darrell, Yong Lee, and Jakob Foerster. Risks and Opportunities of Open-Source Generative AI, May 2024.

[68] Directive (eu) 2019/790 of the european parliament and of the council of 17 april 2019 on copyright and related rights in the digital single market and amending directives 96/9/ec and 2001/29/ec, 2019. Accessed: 2024-09-08.

[69] Zuzanna Warso, Maximilian Gahntz, and Paul Keller. Sufficiently detailed? a proposal for implementing the ai act's training data transparency requirement for gpai, June 2024. This report is published under the terms of the Creative Commons Attribution License.

[70] A. Zhang. *High Wire: How China Regulates Big Tech and Governs Its Economy*. Oxford University Press, 2022.

[71] Matt Sheehan. Tracing the roots of china's ai regulations. *Carnegie Endowment for International Peace*, February 2024. Accessed May 2, 2024.

[72] G. Webster, J. Zhou, M. Shi, H. Dorwart, J. Costigan, and Q. Chen. Forum: Analyzing an expert proposal for china's artificial intelligence law. *DigiChina, Stanford University*, August 2023. Accessed May 2, 2024.

[73] China Money Network. Chinese tech giants dominate ai algorithms with a focus on industry-specific applications. *China Money Network*, March 2024. Accessed May 2, 2024.

[74] Huggingface.co. Models, May 2024. Accessed May 2, 2024.

[75] ChinaTalk. Hugging face blocked! 'self-castrating' china's ml development + jordan at apec. *ChinaTalk*, October 2023. Accessed May 2, 2024.

[76] The State Council of the People's Republic of China. Made in china 2025, 2015. Accessed May 2, 2024.

[77] Congressional Research Service. The made in china 2025 initiative: Economic implications for the united states, April 2019. Accessed May 2, 2024.

[78] Global Times. China to develop 10,000 'little giants' in push for advanced manufacturing. *GlobalTimes.cn*, July 2021. Accessed May 2, 2024.

[79] Angela Huyue Zhang. How china regulates big tech and governs ai, March 2024. Philip K.H. Wong Centre for Chinese Law [Video]. YouTube. Accessed May 2, 2024.

[80] Zeyi Yang. Why the chinese government is sparing ai from harsh regulations—for now. *MIT Technology Review*, April 2024. Accessed May 2, 2024.

[81] Caixin Global. Full text: Xi jinping's speech on boosting common prosperity. *Caixin Global*, October 2021. Accessed May 2, 2024.

[82] Bloomberg News. In its latest crackdown, china intensifies focus on real estate. *Aljazeera.com*, July 2021. Accessed May 2, 2024.

[83] Giulia Intresse. China's new draft regulations for after-school tutoring. *China-Briefing.com*, February 2024. Accessed May 2, 2024.

[84] Lulu Yilun Chen and Li Liu. China ends tech crackdown with fines on tencent, ant group. *Bloomberg.com*, July 2023. Accessed May 2, 2024.

[85] International Monetary Fund. World economic outlook: April 2024, April 2024. Accessed May 2, 2024.