NETWORK LAW REVIEW

ARTICLE

Artificial Intelligence and Data Policies: Regulatory Overlaps and Economic Tradeoffs

Ginger Zhe Jin, Liad Wagman & Mengyi Zhong

The Network Law Review is pleased to present a special issue entitled "The Law & Technology & Economics of AI." This issue brings together multiple disciplines around a central question: What kind of governance does AI demand? A workshop with all the contributors took place on May 22–23, 2025, in Hong Kong, hosted by Adrian Kuenzler (HKU Law School), Thibault Schrepel (Vrije Universiteit Amsterdam), and Volker Stocker (Weizenbaum Institute). They also serve as the editors.

Abstract. Advances in artificial intelligence (AI) have sparked intense policy debates worldwide on whether and how to govern the technology. Because data is an input into the training of modern AI systems, existing data regulations may intersect with AI policy proposals. Jurisdictions worldwide have developed distinct regulatory frameworks for governing data, including its privacy and security. These frameworks can also increasingly shape the trajectory of AI innovation and deployment. We examine how international data regulations intersect with emerging AI policies. We then highlight some of the economic trade-offs in terms of balancing competition and innovation against potential policy restrictions, and suggest directions for potential policy consensus.

***

1. Introduction

Governments around the world are actively developing or considering AI policies to balance technological advancement with regulatory safeguards. The global landscape of AI governance is highly fragmented, reflecting diverse legal, economic, and political priorities across jurisdictions. While most countries have yet to

implement comprehensive AI legislation, many have introduced regulatory frameworks and guidelines that apply to AI within specific sectors.

The Artificial Intelligence Act, adopted by the European Union (EU) in 2024, is the first major legal framework governing AI. The act introduced a risk-based approach to AI regulation, categorizing AI systems based on their potential for harm. The emergence of ChatGPT in late 2022 led to significant revisions to the Act to accommodate generative AI and general-purpose AI systems, as the new developments challenged the Act's initial risk categorization framework. While the risk categories specified in the EU's AI Act are conceptually clear, the precise mapping of use cases may not be simple in practice. As of the time of this writing, MIT's AI Risk Repository has identified 777 risks in total, highlighting significant gaps in existing risk frameworks, with the average framework covering only 34% of the identified risk subdomains.[1]

In contrast, China and the United States have taken more targeted, sector-specific approaches. China regulates AI incrementally, imposing distinct rules on specific applications, such as algorithmic recommendations, deep synthesis, and generative AI services. The U.S. has adopted a decentralized, sector-driven model. While there is no federal AI law, President Biden's Executive Order on Safe, Secure, and Trustworthy Artificial Intelligence was issued on October 30, 2023, rescinded on January 20, 2025, and subsequently replaced by a new executive order titled "Removing Barriers to American Leadership in Artificial Intelligence" (Executive Order 14179) on January 23, 2025.[2] This new directive aims to promote AI development free from ideological bias, enhance economic competitiveness, and maintain national security by revoking certain existing AI policies perceived as hindrances to innovation. In the meantime, enforcement agencies such as the Federal Trade Commission (FTC) apply existing consumer protection laws, like Section 5 of the Federal Trade Commission Act (against unfair or deceptive practices), to address AI-related misconduct. Meanwhile, state-level regulations are proliferating, focusing on areas such as bias and discrimination, facial recognition, and deepfake technology. According to the National Conference of State Legislatures, as of early 2025, 45 U.S. states and three territories have introduced AI-related legislation, with 31 states and two territories successfully enacting laws.[3]

[1] https://ide.mit.edu/insights/mit-researchers-create-an-open-ai-risk-repository/

[2] Initial rescissions (Jan 20, 2025): https://www.whitehouse.gov/presidential-actions/2025/01/initial-rescissions-of-harmful-executive-orders-and-actions/ | Executive Order 14179 (Jan 23, 2025): https://www.whitehouse.gov/presidential-actions/2025/01/removing-barriers-to-american-leadership-in-artificial-intelligence/

[3] https://www.ncsl.org/technology-and-communication/artificial-intelligence-2024-legislation

Beyond regulations aimed at protecting consumers from AI-related fraud, there is a growing global consensus on the need to safeguard children's privacy, particularly in relation to AI-driven technologies. Regulatory frameworks across jurisdictions share common principles, including parental consent requirements, data minimization, restrictions on profiling, and transparency obligations. In the U.S., the FTC enforces the Children's Online Privacy Protection Act (COPPA) and has taken enforcement actions against companies such as YouTube for AI-driven behavioral tracking on children's content.[4] Similarly, the EU's GDPR-K extends protections to children under 16 (or 13 in some member states), entailing stricter safeguards for AI systems processing children's data.[5] The United Kingdom (UK) goes further by prohibiting manipulative design techniques, requiring AI-powered platforms to default to high privacy settings for children. Companies such as TikTok and Meta have faced regulatory scrutiny in the UK over their AI-driven content personalization systems and their impact on young users.[6] In China, the Minor Protection Law (effective June 2021) imposes stringent restrictions on AI-powered recommendation systems, mandates real-name verification, and enforces strict time limits to curb excessive screen time for minors. Companies like Tencent and ByteDance have responded by implementing "youth mode" features to comply with these regulations.[7]

Overall, there is an increasing global push for structured AI regulations. Beyond the EU, China, and the U.S., other major economies are also advancing AI governance initiatives. India has established a dedicated task force to assess the ethical, legal, and societal implications of AI. Canada is closely aligning its regulatory strategy with the EU's risk-based model, while Japan and South Korea are refining industry-specific AI guidelines. Based on the OECD's national policy database, more than 70 nations are developing over 1,000 policy initiatives related to AI.[8]

The increasing intersection of AI with legal frameworks is also evident in high-profile regulatory interventions (Agrawal et al., 2025). For example, San Francisco banned the use of facial recognition AI by law enforcement due to privacy concerns, while Nevada imposed an excise tax on autonomous vehicle networks to address AI-driven disruptions in transportation.[9] In the realm of intellectual property, the New York Times lawsuit against OpenAI—alleging unauthorized use of its content for AI training—illustrates how copyright law is becoming a central battleground in AI

[4] https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa
[5] https://gdpr-info.eu/art-8-gdpr/
[6] https://ico.org.uk/.../childrens-code-guidance-and-resources/introduction-to-the-childrens-code/
[7] http://en.npc.gov.cn.cdurl.cn/2020-10/17/c_674690.htm
[8] https://www.oecd.org/en/topics/sub-issues/ai-principles.html
[9] SF ban: https://www.nytimes.com/2019/05/14/us/facial-recognition-ban-san-francisco.html | Nevada excise tax: https://law.justia.com/codes/nevada/chapter-372b/statute-372b-145/

regulation.[10] Additionally, the U.S. Copyright Office's recent reports on copyright, artificial intelligence, digital replicas, and the copyrightability of AI-assisted content underscores the legal complexities surrounding AI in content creation and distribution.[11] As generative AI reshapes creative industries, the adaptation of copyright law to address hybrid authorship is essential for safeguarding creative expression, sustaining industry viability, and enabling market opportunities (Cooper et al., 2024). More generally, as AI technology continues to evolve, governments and institutions face the challenge of balancing innovation, competition, and ethical oversight. This paper provides a brief overview of some of the ways that existing data privacy and security regulations may influence AI governance and the economic trade-offs associated with AI governance, while exploring the evolving regulatory landscape across key jurisdictions.

2. Data Regulation and AI

Recent developments in AI have sparked discussions about the importance of data in model performance. Evidence suggests that smaller models can sometimes outperform larger models, challenging the assumption that larger datasets and increased computing power consistently yield better results. More specifically, more than five years ago, Bajari et al. (2019) studied how dataset size affects forecasting accuracy by examining variations in product numbers and time periods available for sale. They find diminishing returns to scale, indicating that while larger datasets do improve accuracy, each incremental increase provides progressively smaller benefits.

More recently, derivative models built upon foundational open-source large language models (LLMs), such as ChatGPT, demonstrate that smaller, specialized models can surpass their base counterparts in specific tasks. For example, performance benchmarks indicate that derivative models like DeepSeek can outperform some ChatGPT models in mathematics and coding tasks.[12] However, according to TrackingAI.org, foundational base models generally still outperform derivative models overall. Since training these base models inherently requires vast amounts of data, the critical role of extensive datasets remains evident. Indeed, recent analyses highlight a dramatic surge in dataset sizes used for training state-of-the-art AI models.[13]

[10] https://www.nytimes.com/2023/12/27/business/media/new-york-times-open-ai-microsoft-lawsuit.html

[11] Part 1: https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-1-Digital-Replicas-Report.pdf | Part 2: https://www.copyright.gov/ai/Copyright-and-Artificial-Intelligence-Part-2-Copyrightability-Report.pdf

[12] https://www.geeksforgeeks.org/deepseek-vs-chatgpt/

[13] https://futuretech.mit.edu/news/what-drives-progress-in-ai-trends-in-data

The dynamic nature of data necessitates continual learning (also known as continuous machine learning or CML). Continual learning allows AI models to adapt by incrementally incorporating new data without complete retraining, further underscoring the ongoing importance of data as a foundational input for sustained AI performance. In short, the evolving relationship between compute and performance complicates efforts to base risk regulation exclusively on compute thresholds. (Hooker, 2024; Schrepel and Pentland, 2024).

Furthermore, AI has become increasingly intertwined with access to data, because data plays a key role in AI inferences and model training. As AI continues to evolve, its reliance on vast amounts of data has intensified, making data regulation an undeniable aspect of AI governance. Personal and copyrighted data inevitably become part of the training of AI models. While many existing data protection and copyright laws were not designed to accommodate emerging AI technologies, their provisions are increasingly being applied to AI-related challenges. These dynamics have resulted in complex challenges underpinning property rights and privacy in the age of AI (Farronato, 2025). While AI may not always be explicitly mentioned in existing data regulations, many provisions in current frameworks are highly relevant to its use. We identify several key areas where AI intersects with data regulation frameworks.

2.1. Profiling and Automated Decision-Making

Profiling, which involves processing personal data to analyze or predict an individual's behavior, preferences, or characteristics, has been significantly enhanced by AI's capacity to process large datasets and identify complex patterns. Automated decision-making, powered by AI models, extends profiling by enabling systems to make high-impact determinations—such as approving loans, hiring employees, or setting insurance rates—without direct human intervention.

While the EU's General Data Protection Regulation (GDPR) does not explicitly reference AI, its provisions on automated decision-making (Article 22) have substantial implications for AI systems. The GDPR grants individuals the right not to be subject to decisions based solely on automated processing if such decisions produce legal or similarly significant effects. Organizations utilizing AI-driven decision-making are required to provide meaningful information about the logic involved, with the intent of regulation to enhance transparency and accountability.

Regulatory enforcement actions illustrate how existing data protection laws have been applied to AI-related cases. For example, the Berlin Commissioner for Data Protection and Freedom of Information fined a financial institution for using AI-generated credit scores in a non-transparent manner, violating GDPR transparency

requirements.[14] Similarly, Italy's Data Protection Authority imposed a €15 million fine on OpenAI, citing inadequate transparency in data collection and insufficient safeguards for minors using ChatGPT.[15] Other notable cases include the French Data Protection Authority's enforcement actions against Clearview AI for unlawful facial recognition practices,[16] and the Dutch Supervisory Authority's penalties against an AI-driven fraud detection system for GDPR violations (Clark et al., 2024).[17]

Beyond the EU, several other jurisdictions have adopted regulatory provisions that, while not explicitly framed as AI regulations, impose constraints on automated decision-making and AI-driven profiling. China's Personal Information Protection Law (PIPL) requires explicit consent for AI-powered automated decisions that significantly affect individuals. South Korea's Personal Information Protection Act (PIPA) also mandates consent and provides individuals with mechanisms to contest AI-driven decisions. In contrast, the U.S. regulatory landscape remains fragmented. While no federal law comprehensively regulates AI profiling, state-level laws such as the California Consumer Privacy Act (CCPA) and the Colorado Privacy Act (CPA) grant individuals the right to opt out of certain AI-driven decision-making processes. Additionally, jurisdictions like New York, Illinois, and Colorado have introduced more targeted regulations, particularly in high-risk areas such as employment and financial services.[18]

Data anonymization techniques, previously considered adequate for privacy protection against conventional algorithms, are now increasingly susceptible to AI-driven de-anonymization attacks (Yang et al., 2024). Emerging AI algorithms can analyze massive datasets, identifying connections and patterns at significantly lower marginal cost and with greater accuracy than traditional algorithms. This capability undermines established privacy protections, as even with the removal of obvious identifiers, AI may re-identify individuals using seemingly innocuous data points like location history, shopping habits, and social media activity. This trend is prompting policymakers and organizations to reassess and update data protection strategies to address such challenges and comply with regulations such as the EU's GDPR and China's PIPL, which allow for truly anonymized data (data that cannot be

[14] https://www.edpb.europa.eu/.../berlin-sa-imposes-300-000-euro-fine-against-bank-after-lack-transparency_en

[15] https://www.reuters.com/.../italy-fines-openai-15-million-euros-over-privacy-rules-breach-2024-12-20/

[16] https://www.edpb.europa.eu/.../french-sa-fines-clearview-ai-eur-20-million_en

[17] https://www.edpb.europa.eu/.../dutch-supervisory-authority-imposes-fine-clearview-because-illegal-data_en

[18] NYC Local Law 144: https://www.nyc.gov/site/dca/about/automated-employment-decision-tools.page | Illinois HB3773: https://www.ilga.gov/.../DocNum=3773&GAID=17 | Colorado SB24-205: https://leg.colorado.gov/bills/sb24-205

used to identify a specific person) to be shared for research and commercial purposes.[19]

2.2. Consent as a Legal Basis

Consent serves as a fundamental legal basis for data processing in most regulatory frameworks, but its application to AI presents several challenges. One key issue is the scope and purpose of consent. Individuals typically provide consent for specific, well-defined uses of their data, but AI systems may later repurpose this data for unforeseen applications. For instance, users may share content on social media platforms without realizing that their data might be used for AI model training and/or sold to third parties for that purpose.[20] This disconnect raises concerns about whether an initial consent remains valid for subsequent, unanticipated data uses.

Some jurisdictions have addressed this challenge by requiring renewed consent for new data uses. India's Digital Personal Data Protection Act (DPDPA) mandates fresh consent if data is processed for a purpose not reasonably related to its original use. Similarly, South Korea's PIPA stipulates that if the purpose of data processing changes significantly, organizations must obtain additional consent. However, enforcing such requirements remains difficult, as individuals are often unaware of how their information is utilized beyond its initial collection.

The challenges of relying solely on consent are exemplified in the experiences of public figures. Celebrities often share personal information willingly to engage with their audience. However, this openness can lead to misuse of their data, resulting in harm and privacy violations. For instance, the publicly available voice, likeness, and identity of a celebrity may be exploited for unauthorized endorsements and objectionable content, highlighting the limitations of consent as a protective measure.[21] These instances underscore that even when consent is given, it does not safeguard against all forms of data exploitation. Beyond celebrities, today's consumers mainly navigate their privacy choices through product and product usage selections, but privacy often necessitates an ongoing, active consumer role, including navigating how personal data is shared and interpreted to ensure privacy and other outcomes are aligned with one's interests. Privacy protection is unlikely to be effective unless individual consumers have some say regarding when, how, and with whom their information is shared (Kuenzler, 2021).

---

[19] https://bidenwhitehouse.archives.gov/.../executive-order-on-advancing-united-states-leadership-in-artificial-intelligence-infrastructure/

[20] https://apnews.com/article/reddit-openai-chatgpt-bd2291fcc226bc737a44dbef4a31563f

[21] https://www.theguardian.com/.../indian-actor-anil-kapoor-wins-court-battle-over-ai-use-of-his-likeness

Another issue concerns the implementation of opt-in versus opt-out consent mechanisms. Opt-in models require users to actively provide consent before data collection, ensuring voluntary participation. Conversely, opt-out models assume default consent unless users take action to withdraw it, which may lead to uninformed or involuntary data sharing, as individuals may lack the awareness, technical skills, or time to navigate opt-out processes effectively. Consequently, data collection under opt-out schemes may not reflect genuine user intent.

2.3. Data Localization and Cross-Border Transfers

AI development depends on large, diverse datasets, making cross-border data flows essential for training and optimizing AI models. However, data localization laws—which mandate that certain types of data be stored within national borders—pose significant challenges to AI development. Countries such as China, India, and Russia enforce strict domestic data storage requirements, while the U.S. has implemented Executive Order 14117, restricting the transfer of sensitive personal and government-related data to designated foreign jurisdictions.[22]

The U.S. Framework for Artificial Intelligence Diffusion adopted by the U.S. Department of Commerce's Bureau of Industry and Security in January 2025 aims to balance AI leadership, security, and controlled global dissemination. It introduces export controls on AI chips and non-public model weights, classifying countries into three tiers: Tier 1 (U.S. and key allies, unrestricted access), Tier 2 (most nations, restricted exports), and Tier 3 (arms-embargoed countries, full restrictions). The framework caps AI chip deployment in Tier 2 countries, mandates security safeguards (cybersecurity, physical security, vetted personnel), and restricts advanced model weight access. While mitigating risks of alternative AI ecosystems, the long-term goal is to preserve U.S. and allied dominance in AI innovation and infrastructure.[23]

A prominent example of the impact of data localization laws is Tesla's operations in China. Since 2021, Chinese regulations have required Tesla to store all vehicle-generated data within the country, prohibiting its transfer abroad without government approval. This has complicated Tesla's development of autonomous driving technologies, which rely on extensive, cross-border datasets. To comply with local regulations, Tesla has built data centers in Shanghai, but further challenges have

[22] Federal Register (EO 14117 background): https://www.federalregister.gov/.../preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related
[23] https://www.rand.org/pubs/perspectives/PEA3776-1.html

emerged due to U.S. restrictions on overseas AI model training under the Biden administration's Framework for Artificial Intelligence Diffusion.[24]

To balance national security concerns with the need for global AI collaboration, some jurisdictions are introducing regulatory exemptions for certain types of data transfers. In March 2024, China amended its cross-border data transfer rules, allowing exemptions for datasets involving fewer than 100,000 individuals or those processed for contractual or human resources purposes.[25] Despite these regulatory adaptations, multinational AI companies continue to face complex compliance landscapes that can hinder innovation.

The growing scrutiny of cross-border data flows also extends to AI applications developed by foreign companies. For instance, the Chinese AI company DeepSeek has faced regulatory restrictions in multiple countries due to concerns over data privacy and security. South Korea's Personal Information Protection Commission temporarily suspended new downloads of DeepSeek, citing non-compliance with national data protection laws.[26] These cases underscore the increasing role of data governance in shaping AI policy at both national and international levels.

These developments suggest a trend toward balancing national security interests with the demands of global AI advancement, potentially offering new avenues for cross-border AI development and deployment strategies. As AI technologies continue to advance, regulatory frameworks will need to evolve to address the intersection of AI, data protection, and privacy, while balancing innovation with consumer rights and security.

3. AI Policy Evolution and the Path Ahead

As AI becomes increasingly embedded in global economies and societies, governments are leveraging data and AI policies and regulations as both a protective measure and a strategic tool.

On the protective side, a number of existing laws already govern manufacturers' liability in product flaws and misuse. However, unlike chainsaw manufacturers who can largely avoid liability in misuse by providing proper warnings on product labels, AI tools blend development, deployment, and decision-making in a way that blurs

[24] https://www.nytimes.com/2025/02/25/business/china-tesla-self-driving-musk.html
[25] https://iapp.org/news/a/chinas-new-cross-border-data-transfer-regulations-what-you-need-to-know-and-do
[26] https://www.reuters.com/.../south-koreas-data-protection-authority-suspends-local-service-deepseek-2025-02-17/

the lines of product responsibility. As described above, AI tools also involve large-scale, and potentially continual, use of individual data, raising consumer protection issues (such as privacy and data security) well beyond traditional product liability. How to craft a liability regime that incentivizes safe AI innovation while deterring AI misuse is one of the major challenges facing policymakers.

On the strategic side, a growing trend involves imposing stricter compliance requirements on foreign enterprises while offering more lenient conditions for domestic firms. This approach is evident in the U.S., where the government has implemented restrictions on China's access to high-performance computing chips to preserve its technological edge. Following the emergence of advanced AI models from DeepSeek, U.S. policymakers moved to further block China from obtaining AI chips through third-party nations, reinforcing broader geopolitical efforts to preserve AI leadership.

Either protective or strategic, the influence of regulation on AI innovation is becoming more pronounced. Research suggests that stringent data laws, such as the GDPR, may have prompted firms with significant exposure to the EU market to shift toward AI innovations that rely less on user-generated data. However, it has been argued that such practices may have slowed innovation in terms of reducing overall AI patenting activity, and that data regulations have also reinforced the dominance of established technology companies (Frey et al., 2024). A related literature has documented the impact of GDPR on market concentration (Peukert et al., 2022; Johnson et al., 2023), technology venture investments (Jia et al., 2021; Jia et al., 2025), and app innovations (Janßen et al., 2022).[27] There is a risk that AI regulations, unless carefully formulated, could have similar effects, since compliance costs entail non-negligible fixed costs, which can be relatively high for smaller, younger and more resource-constrained firms. More generally, while the EU's AI Act may prevent market fragmentation, it raises entry barriers and distorts competition (Schrepel, 2025). These dynamics illustrate the complex trade-offs between regulatory oversight and competition that drives innovation.

Beyond economic and geopolitical considerations, there are emerging security risks. The rapid advancement of borderless fraud linked to AI and digital currencies, including AI-generated phishing scams, deepfake impersonations, romance fraud, and other forms of automated and semi-automated financial fraud, has outpaced existing prevention and deterrence mechanisms. Malicious entities can increasingly leverage current and emerging technologies to create sophisticated scams that are

[27] See Johnson (2024) for a broader review of GDPR effects and Jin & Wagman (2021) on overlaps between antitrust and consumer protection.

difficult to detect, raising significant concerns about consumer protection. While many data and AI legislations focus on regulating legitimate firms that then need to expend time and resources to comply, scammers and fraudsters may completely ignore such regulations unless they are actively enforced with sufficient deterrence and prevention. Viewed in this way, insofar as deterrence, the enforcement of policy with respect to scams and fraud may yield a high return on regulatory effort.

Moreover, enforcement may trigger existing anti-human trafficking and white-collar fraud laws. AI-generated scams, such as deepfake impersonations and cryptocurrency schemes, have been linked to human trafficking networks where victims are coerced into operating fraud operations.[28] In such cases, authorities could apply anti-trafficking laws like the U.S. Trafficking Victims Protection Act and the UN Protocol to Prevent, Suppress and Punish Trafficking in Persons. Financial crimes involving AI, including investment fraud, phishing, and identity theft, could also be prosecuted under white-collar statutes such as the U.S. Wire Fraud Act, the Securities Act of 1933, and the UK Fraud Act 2006. If AI-driven scams are linked to organized crime, the RICO Act in the U.S. could enable broader prosecution of criminal enterprises. Given the cross-border nature of AI-related fraud, international frameworks like the Budapest Convention on Cybercrime and Interpol's Cybercrime Directorate may facilitate cooperation among jurisdictions.

However, AI and data-related regulatory enforcement cases have primarily concentrated on issues such as insufficient legal basis for data processing, non-compliance with general data processing principles, and inadequate technical and organizational measures to ensure information security.[29] While such oversight serves important purposes, enforcement agencies would benefit from strengthening actions against AI-facilitated criminal activities. This includes developing targeted regulations to restrict criminal access to AI technologies and fostering the development of resources, such as AI watermarking technologies, to enable origin tracing. Strengthening these areas of focus could help reduce the growing use of AI by bad actors to conduct and expand illicit activities. Unlike legitimate firms that invest in regulatory compliance, criminal actors operate outside of established regulatory frameworks. Therefore, enhancing enforcement and deterrence mechanisms for AI-facilitated crime would complement existing regulatory approaches and potentially reduce harmful activities that currently receive less regulatory scrutiny.

[28] https://apnews.com/article/myanmar-thailand-scam-centers-trapped-humanitarian-c1cab4785e14f07859ed59c821a72bd2

[29] https://www.forbes.com/sites/douglaslaney/2024/06/12/gdpr-violations-and-fines-trends-insights-and-compliance-strategies/

Addressing these challenges may require internationally coordinated efforts to develop standardized frameworks, given the borderless nature of scams and fraud. Without such coordination, illicit actors will likely exploit regulatory gaps by operating from jurisdictions with weaker oversight.[30] To that end, governments should foster collaboration to improve fraud detection and deterrence mechanisms, while AI developers should implement safeguards such as authenticity verification tools and watermarking systems for AI-generated content. The global nature of AI-driven scams underscores the need for an internationally coordinated regulatory response to protect consumers.

As regulatory frameworks evolve, there is a growing tension between oversight and innovation. While AI policies may aim to enhance transparency, accountability, and safety, overly restrictive regulations can inadvertently hinder technological progress or drive companies to relocate to jurisdictions with fewer compliance burdens. A notable example is the Dutch software firm Bird, which recently announced plans to shift its operations outside of Europe, citing restrictive AI regulations and difficulties in hiring skilled AI professionals.[31] This trend highlights the "free-rider" problem in AI development, where firms operating in regions with more lenient regulations can advance their AI models with fewer constraints, potentially gaining a competitive edge over those in more regulated markets. The ability of these companies to subsequently introduce AI models into highly regulated regions raises concerns about the effectiveness of local compliance measures and the competitive landscape of AI innovation. The Bird case also underscores the trade-off between omnibus (e.g., the EU's AI Act) and sector-specific regulations (e.g., developed by regulatory bodies such as the FAA for aviation, the SEC in finance, and the DHHS in healthcare). While omnibus regulations can be burdensome for the private sector and miss the areas that need regulations most, sector-specific AI regulations can face ambiguous sector classifications and may generate conflicting requirements across sectors.

The future of AI governance stands to be shaped by ongoing technological advancements, economic shifts, and geopolitical realignments. Policymakers must navigate the challenge of balancing AI regulations across jurisdictions while accounting for national security interests and the need for global collaboration. Greater regulatory cooperation among major economies can help reduce fragmentation and free-riding. At the same time, fostering transparency and accountability within AI systems will require the adoption of explainability

[30] https://apnews.com/article/myanmar-online-scam-centers-myawaddy-trafficking-china-thailand-9fce90b60eb8cf5a42569f0e7ec865f6

[31] https://www.reuters.com/.../dutch-software-firm-bird-leave-europe-due-onerous-regulations-ai-era-says-ceo-2025-02-24/

measures, such as model documentation and auditing, and subsequent detection mechanisms, in order to enhance trust and reduce fraud. By addressing these challenges proactively, governments can create regulatory environments that safeguard consumer rights, mitigate risks, and promote AI-driven economic growth without stifling progress.

In doing so, policymakers must balance the need for regulatory oversight with the imperative to foster AI-driven innovation. The fragmented and evolving landscape of AI regulation underscores the need for a balanced approach that promotes innovation while safeguarding individual rights and promoting accountability. Although full international coordination on AI regulation is unlikely due to strategic competition and differing national interests, selective cooperation in areas with broad consensus—such as AI-driven fraud prevention, algorithmic transparency, and child protection—offers a more achievable path. Expanding existing data regulations to address AI-specific challenges, rather than creating entirely new frameworks, could improve regulatory efficiency while minimizing compliance burdens. However, certain AI-related risks, including automated decision-making, may require distinct, AI-focused policies that build on but remain separate from data regulations. Free-riding, where firms exploit gaps in global regulatory alignment by developing AI in jurisdictions with weaker oversight, is set to remain in place without a degree of international coordination on baseline standards. By focusing on high-impact, low-resistance areas of consensus and adopting a hybrid regulatory approach, policymakers can strike some balance between encouraging AI-driven innovation that avoids disproportionately burdening smaller firms and entrants, and ensuring responsible deployment. Ultimately, navigating these complex trade-offs will require dynamic and adaptive governance models that reflect the rapidly evolving nature of AI technologies and their societal impacts.

Given the rapid pace of AI advancement and the current uncertainty regarding its societal impacts, formulating concrete regulatory recommendations remains challenging. Instead, we point to three directions for potential policy consensus. First, international collaboration is critical for developing coherent AI governance frameworks that facilitate cross-border compliance, particularly in protecting children and preventing transnational fraud. Second, rather than constructing entirely new regulatory regimes, it may be more practical and effective to adapt and extend existing legal instruments, such as those governing consumer protection, privacy, and competition, to meet AI-specific challenges through targeted amendments, adaptations, and interpretive guidance. Third, there is a pressing need to support the collection and dissemination of accurate, timely, and comprehensive data on the benefits and risks of AI. Ensuring broad access to this information via

both centralized and decentralized mechanisms would enable evidence-based regulation and foster market-based accountability among AI developers and users.

Recent global efforts such as the Singapore Consensus on Global AI Safety Research Priorities are aligned with one or more of these directions. Developed through collaboration among over 100 international researchers, the Singapore Consensus highlights the potential to use prospective risk analysis and structured analytical techniques to assess a variety of yet-to-occur risks, similar to their successful use in nuclear safety, cybersecurity, and aircraft flight control (Singapore Consensus, 2025). Integrating these techniques with accurate, timely and comprehensive data on an ongoing basis would be productive for future AI regulations and global coordination. As AI capabilities advance rapidly, even limited alignment on key safeguards in areas such as child protection and fraud prevention can reduce systemic vulnerabilities without requiring full harmonization across legal regimes.

Ginger Zhe Jin, Liad Wagman &
Mengyi Zhong

***

* We are grateful for the financial support from the International Center for Law and Economics (ICLE). Jin and Wagman worked full-time at the US Federal Trade Commission in 2015–2017 and 2020–2022, respectively. Wagman is an academic affiliate at the International Center for Law & Economics (ICLE). Jin was on academic leave to work full-time at Amazon from 2019 to 2020. Both Jin and Wagman have provided consulting services to a few companies in the areas covered by this article. All opinions and errors are our own. All rights reserved.