IJHSR
ijhighschoolresearch.org
REVIEW ARTICLE

A Comprehensive Review of AI Regulations and Their Effects on Innovation and Adoption

Ryan Chen

Millburn High School, 462 Millburn Ave, Millburn, NJ 07041, USA; ryansjchen@gmail.com

ABSTRACT: Society stands on the precipice of a new technological era with Artificial Intelligence (AI) transforming numerous industries and becoming increasingly integral to society. Generative AI, defined as models that can produce human-like content (e.g., text or images) by learning from large datasets, has significantly expanded the capabilities of AI. In response to this development, legacy legal doctrines are being reinterpreted and applied to the unique challenges posed by generative AI systems. Simultaneously, regulatory bodies have introduced governance frameworks that seek to align innovation with ethical, legal, and societal safeguards. This paper aims to provide a detailed synthesis of both legacy and emerging governance frameworks, evaluating their influence on the pace and direction of innovation in generative AI. First, I examine how legacy doctrines such as Data Protection, Intellectual Property, Liability, and Intermediary Liability apply to generative AI. Then, I consider regulatory proposals for AI from various governments. Finally, I evaluate the impact that regulation could have on the innovation and adoption of AI. This paper aims to provide a reference for policymakers and researchers, while also encouraging more discussion on how to sensibly approach AI regulation..

KEYWORDS: Systems Software, Algorithms, Generative AI, Governance, AI Innovation.

Introduction

The rise of Generative Artificial Intelligence marks an inflection point where computational creativity has begun to match human ingenuity. Unlike earlier predictive models that simply classify or rank existing data, generative systems produce new text, images, code, and audio, expanding the scope of automation and challenging the rationale that served as the foundation for current AI policy.[1] These generative AI tools, such as ChatGPT, Claude, or Gemini, are the product of the substantial investment in recent years that has accelerated progress in machine learning and deep learning. For instance, venture capital funding for generative AI start-ups has increased by more than 74 percent since 2017, signaling strong confidence in a technology that now reaches millions of users globally.[2] With this rapid growth, generative AI can have a profound impact on our global economy in the long term, potentially adding between 2.6 and 7.9 trillion US dollars to global output each year.[2] At the same time, nearly forty percent of jobs are vulnerable to automation, with inequality likely to intensify without large-scale programs for reskilling and social protection.[3-5] Beyond economic consequences, it is important to discuss the widening spectrum of societal risks surrounding realistic deepfakes, intellectual property rights, algorithmic bias, and the spread of misinformation.[6-8] These risks raise concerns for national and individual security, as manipulated media can distort democratic processes and incite violence, while biased algorithms may entrench discrimination in employment, financial systems, or law enforcement. Moreover, there are concerns that without proper guardrails, generative AI can enable pervasive state-run surveillance, concentrate power in a few firms, or give rise to highly autonomous systems that escape human oversight.[9]

Given the scale of these risks, policymakers increasingly acknowledge that current regulatory frameworks are no longer sufficient. Designing effective rules for AI has therefore become both essential and unusually complex because the underlying technologies evolve rapidly while their harms and benefits cut across many domains.[10] As a result, courts and legislatures have begun to apply legacy doctrines, including Section 230, liability, and copyright law, to cover autonomous content creation.[11-14] However, debates persist over whether incremental regulation can keep pace or whether entirely new legal frameworks are required. Alongside these debates, governments and international bodies have introduced dedicated frameworks such as the European Union's Artificial Intelligence Act, China's Interim Measures for Generative AI Services, and the United States' AI Action Plan.[13-15,17] Additionally, international organizations such as the OECD, UNESCO, the G7, and the Council of Europe have also developed frameworks for AI regulation.[15-17] However, despite the rapid proliferation of regulatory initiatives across jurisdictions, substantial gaps remain, with current scholarly frameworks collectively addressing only about thirty-four percent of the risks identified by bodies such as NIST, the European Union, and ISO.[18] To address these gaps, scholars over the past few years have proposed a range of regulatory approaches, with some outlining their own frameworks, and others synthesizing global policies into one harmonized plan intended to capture the full spectrum of risks and opportunities presented by generative AI.[19-21] However, a clear gap in the literature remains regarding how current legal doctrine and emerging global regulation affect technological development and innovation. Thus, this paper evaluates the current state of generative AI governance by surveying research on legacy frameworks, newly developed generative AI policies,

DOI: 10.36838/IJHSR811.228

and empirical analyses of innovation. By reviewing these studies, this paper aims to guide future policymaking that balances innovation with safeguards, promoting further dialogue surrounding how to ensure the proper regulation of generative AI. Considering the economic promise of generative AI alongside its potential to deepen inequality and heighten security risks, it is essential to design regulations that mitigate harm without stifling progress. In the next sections, this paper will first review how foundational legal doctrines, including data protection, copyright, liability, and intermediary liability, are being reinterpreted to govern generative AI models. Then this paper will survey the statutes, regulations, and policies introduced by national governments. Finally, this paper reviews how regulations influence innovation, investment, and adoption of AI.

Discussion

1. Legacy Legal Doctrines:

Legacy legal doctrines are increasingly being applied to the challenges posed by generative AI, raising important questions about whether AI falls within the scope of these doctrines and whether they remain effective in practice. Although many of these doctrines are not AI-specific, they are still extremely influential on the trajectory of AI development and deployment, as both insufficient regulation and overregulation of these legacy doctrines could have profound consequences for innovation and individual rights.[9] This section reviews the literature surrounding how different jurisdictions are applying legacy doctrines to AI, with a primary focus on the United States and the European Union, as well as China, for areas where its framework is especially relevant, such as data protection and intellectual property. To reflect the different structures of these countries, the review will be organized by country for data protection, liability, and intermediary liability, while intellectual property will be broken down thematically, given its two distinct questions of training and authorship.

1.1. Privacy and Data Protection:

One of the most impactful and controversial issues in generative AI is how AI training interacts with privacy and data-protection laws. Generative AI models are typically trained on three types of data: (1) information that is publicly available on the internet, (2) data that the developer licenses from third parties, and (3) the data provided by human trainers or users.[22,23] Information being publicly available does not remove its status as personal data, since all major definitions of personal data in the U.S., EU, and Chinese law agree that such data remains protected.[23-25] In this section, we will be discussing how comprehensive current data-protection laws are addressing AI, focusing on the approaches of the United States, the European Union, and China. It should be noted, however, that this section focuses on overall regulatory frameworks or environments, rather than sector-specific rules, which can impose even stricter regulations in industries such as healthcare.[26]

1.1.1. United States

The United States lacks a comprehensive federal privacy and data protection law, with protections being sector and state-specific.[22,26,27] The most prominent state statute is California's CCPA, which requires businesses to inform consumers of the categories of data collected, the purposes for collection, and how that data will be managed.[22,26,27] Consumers may request information about their data, seek correction or deletion, know what information is shared and with whom it is shared, and opt out of storage, retention, or transfer of their data.[26] Although the statute does not explicitly state AI, it applies to organizations that develop or use AI trained on large consumer datasets, and recent revisions add duties to disclose appropriate uses of automated decision systems to users, to conduct risk assessments that describe safeguards to ensure appropriate use, and to refrain from processing data when privacy risks outweigh benefits to society.[22,26] At the federal level, the Federal Trade Commission (FTC) uses Section 5 to police unfair or deceptive data practices and has brought hundreds of these cases to court, though critics have argued that this policing is overreach in certain cases (e.g., *FTC v. Wyndham Worldwide*).[26] For instance, in the cases of Rite Aid and Alexa, the FTC ordered the deletion of unlawfully obtained data along with the algorithms and models built from it.[22] Across the AI lifecycle, Fair Information Practice Principles such as data minimization and purpose limitation restrict repurposing data collected for one use to train models for another without a new legal basis or a documented compatibility analysis.[22] Overall, despite opt-outs and other rights in state and sector rules, there is a large burden placed on individuals to protect their data.[22] Individuals often do not know when their data has been scraped, brokered, or repurposed for training. Moreover, because federal proposals such as the American Data Privacy Protection Act have stalled, the U.S. landscape for data-protection and privacy remains extremely fragmented, leaving AI developers to navigate overlapping state, sectoral, and federal rules without a single national standard.[22]

1.1.2. European Union's General Data Protection Regulation:

The European Union regulates privacy and data protection through the General Data Protection Regulation (GDPR), which has been applied since 2018 to harmonize national rules and strengthen individual rights.[13,22-24] The GDPR defines personal data broadly as information relating to an identified or identifiable person and gives data subjects rights regarding their personal data. For data collection, there are 6 legal bases outlined in Article 6.[23,24] Many AI providers rely on the legitimate-interests basis, which requires three conditions for processing large amounts of data: (1) a legitimate interest, (2) processing data must be necessary for that interest, and (3) that the interest is not outweighed by the rights and freedoms of the data subject.[23] Many providers' legitimate interest is commercial, which can qualify as legitimate, but even if providers prove that they have a legitimate interest, Article 5 requires that data collection be limited to only what is strictly necessary (i.e., not the entire internet), and that information gathered cannot later be repurposed for objectives beyond those originally specified at the time of collection.[23] Then, in accordance with Article 14, a provider must notify all individuals when their data is collected directly; however, due to the amount of

data collected, providers usually invoke the "disproportionate effort" exception and publish general notices.[23] In principle, if a provider could effectively and permanently anonymize the data (i.e., you cannot reconstruct the original data from the model), the trained model could fall outside of the definition of "personal data" under the GDPR.[23] In practice, however, advanced attacks (e.g., model inversion) can still reconstruct elements of the original non-anonymized training data, which makes achieving anonymization that meets the GDPR's strict standards very difficult.[23,28] Regarding data subject rights, the GDPR provides individuals the right to request access to, information about, and deletion of their data.[22-24] Despite this, those rights are very difficult to enforce because while users could request that their information be deleted from the training dataset, it would be very difficult to trace the data in question, and deletion from the dataset does not remove its imprint from the model's weights, so the information can persist and reappear in outputs.[23]

1.1.3. China:

China's privacy and data-protection policy seeks to protect individual data rights while also safeguarding national security and the public interest.[24,25] China took influence from the EU's GDPR, defining personal data mainly with two doctrines: the Personal Information Protection Law (PIPL), which defines personal data as information that is related to an identified or identifiable natural person, and the Civil Code of the People's Republic of China (CCPRC), which defines it as any information that can identify a person by itself or combined with other information.[24,25,29-31] To connect these older doctrines to the new challenges posed by AI, China passed the AI Measures, which requires high quality training data, and protection of data subjects' rights and interests during development and deployment.[25,32] The AI measures mainly function as a bridge between the older legal system and AI, acting as high-level guidance that mainly tells AI to comply with existing data-protection and privacy laws such as PIPL and CCPRC.[25,32] Similar to the EU, individuals enjoy rights such as to be informed, to give or refuse consent, to access their data, and to seek correction and erasure.[24,25] Specifically, providers must obtain consent from data subjects; explain the scope, purpose, and methods of processing; cooperate with requests to inquire about, copy, or delete data; and safeguard data against breaches.[24,25] Publicly available personal information, however, may be processed without consent within a reasonable scope.[24,25] Moreover, providers are limited to only collecting data that is essential for stated purposes and may not repurpose it for incompatible uses.[24,25] To ensure data is safe, providers are required to encrypt and de-identify data, appoint personal information protection officers, record and keep audits, and allow for external supervision by the government.[25] While there is a heavy priority on the safety of data, victims face difficulties obtaining relief for harms from data leaks due to how vague Article 69 of PIPL is on determining non-material damage.[25]

1.2. Intellectual Property:

Intellectual Property (IP) law protects an author's creative work (e.g., inventions, literary or artistic works, and designs) by granting creators exclusive rights to their works, incentivizing more innovation and creativity.[7,33-35] The introduction of generative AI challenges IP laws, as the training data for generative AI models often includes copyrighted works, and the outputs of generative AI partially contain human contributions.[7,33-35] Unlike the other legal doctrines analyzed in this paper, IP law raises two very distinct questions in the context of AI: training and authorship.[7,33-35] Thus, this section will be organized thematically around these two issues rather than by country, examining whether the use of protected works for AI training is lawful under global IP law frameworks, and whether the outputs of AI systems contain protectable human authorship and, if so, who owns them.

1.2.1. Training Data:

The central issue surrounding IP law and generative AI is whether developers are allowed to use copyrighted works to aid the training of generative AI models without permission from the rights-holder.[13,33-35] Globally, there have been varying levels of regulation and approaches. In the United States, rights-holders challenge the use of these works as unlawful, arguing that using huge numbers of copyrighted works to train models is illegal and not "fair use" because it requires making completely new copies. In response, developers argue that copying is used only to analyze patterns for training and not to replace the works themselves, so therefore it is "fair use."[33,35] Amidst these debates, the US has yet to develop a standardized framework for regulation, relying on the courts to rule on a case-by-case basis.[7,35] To do this, the courts have been relying on the four fair-use factors (purpose, nature, amount, and market effect), and have focused on whether or not the AI is a substitute for the original for its own market.[34] For instance, if the AI output could compete directly with the original work (e.g., stock photos, artwork), then it violates IP law; however, if the copies are just part of the training process and do not have the potential to substitute the originals, the justification for fair use could be stronger.[34,35] Unlike the United States, the European Union has specific legislation addressing the use of copyrighted data for training generative AI models called the "Text and Data Mining Exceptions" from the "Directive on Copyright in the Digital Single Market."[7] Under these rules, as long as the works have been obtained lawfully, developers are allowed to train models with copyrighted works without permission for research uses; however, for commercial uses, it can only occur if rights-holders have not opted out.[7] If the rights-holders have opted out, then the developers must obtain a license to use the work as training data. In China, developers have a larger duty to respect third-party IP. For instance, if copyrighted works are taken to train a model without permission, that is treated as unauthorized copying.[34] Moreover, if the model's output is close to an existing protected work, courts categorize it as a derivative work (i.e., a new work based on or adapted from the original), and require the developer to obtain a license.[34] In the *Ultraman* decision, the Guangzhou Internet

DOI: 10.36838/IJHSR811.228

Court ruled that because the AI-generated image resembled a copyright-protected character, it was deemed a derivative work, and therefore, the developer is expected to remove or license the character for both training and generation.[34]

1.2.2. AI-assisted Authorship:

Across major countries, copyright doctrine continues to revolve around human creativity and authorship. In the United States, fully machine-generated material is not protectable, while AI-assisted works can be protected to the extent of identifiable human creative contribution, with the disclosure of AI's role.[33,34] In the case of the AI-generated comic book *Zarya of the Dawn*, the United States Copyright Office (USCO) protected the human contributions only (e.g., text of the work, the selection, and the arrangement of the images), and required the disclosure of what was made by generative AI, which were the images in this case. In US patent law, the USCO ruled in *Thaler v. Vidal* that an inventor must be human and cannot be AI. In both the European Union and thus the U.K., since they largely follow EU copyright law, works are only recognized as original if the author makes "free and creative choices" and adds a "personal touch."[36] However, unlike the rest of the regulatory regimes, in the UK, there is an exception that allows copyright protection for purely computer-generated works (Section 178 of the UK Copyright Designs and Patents Act), where the "author" is the person making the necessary arrangements for creation; however, this exception has not yet been tested with generative AI.[36]

1.3. Tort Liability:

Tort liability is the body of law that assigns civil responsibility for injuries or harm caused by activities and products, setting the conditions under which victims are compensated and wrongdoers are held liable.[37] Generative AI complicates this framework because many systems function as complex "black boxes," making foreseeability difficult.[38] Thus, the introduction of generative AI raises questions about who should bear responsibility for harmful outputs, whether AI should be treated as a product or a service, and how to evaluate fault when systems appear to act autonomously.[37-42] This section reviews how these challenges are being addressed by existing Tort liability doctrines in the United States and the European Union.

1.3.1. United States' Liability Law:

In the United States, Tort liability is determined on a case-by-case basis, with plaintiffs typically proceeding under one of three main doctrines: negligence, product liability, or strict liability.[37] For negligence, judges evaluate whether a developer has used reasonable care to avoid foreseeable harms to people or property.[37,38,43] Specifically for AI, when deciding if the developer should be held liable, other factors such as a model's societal benefits are considered, as well as if industry standard regulations were followed and if rigorous pre-release testing occurred.[37] In defense, a developer could claim that their model was used by a third-party in an unintended way that resulted in harm.[37,44] However, this defense often does not hold up, because the harm that occurred is usually foreseeable, and thus there should have been safeguards to prevent it from happening.[37] A developer could be shielded, however, if a user substantially alters an AI model or uses it for general advice, and that advice is used for harmful practices (e.g., asking for coding advice that is later used for a cybercrime).[37] Product liability revolves around the manufacture, design, or warnings of a product.[37,42] Whether or not an AI system should be treated as a product is still debated over because software is sometimes treated as a service; however, courts are more willing to treat software embedded in physical devices (e.g., an autonomous car) or certain platform functionalities as products, and the FDA's treatment of software as a medical device supports product characterization in health care.[37,42,45] If an AI system is treated as a product, design-defect claims utilize two tests[37,42,45] First is the risk-utility test, which evaluates whether feasible safeguards or alternative designs would have reduced foreseeable risks without unduly impairing the beneficial uses of the system.[37,42,45] Second is the consumer-expectations test, which holds the developer liable if the product fails to perform as safely as an ordinary customer would expect, and thus causes harm.[37,42,45] This test offers a more specific, plaintiff-friendly path, as plaintiffs using consumer expectations do not have to prove negligence, but this test is overruled by adequate warnings from the developer.[37,42,45] However, while adequate warnings can defeat consumer-expectations claims, failure-to-warn can support the plaintiff without proof that a better warning would have changed user behavior.[37] If a developer releases a system as open-source without warning that fine-tuning can disable built-in safeguards, and a user fine-tunes it, inadvertently removing those safeguards, the developer could be held liable for the resulting harms due to a failure to warn.[37] Some developers argue that open-source systems are a distinct product category that limits design-defect exposure, but ordinary negligence analysis still applies regardless of that classification.[37] Strict liability applies when an actor engages in an abnormally dangerous or ultrahazardous activity (e.g., use of explosives) and causes harm to another person's body or property, regardless of whether the actor exercised all due care or not.[37,46] In the context of AI, it is a possibility that releasing very powerful AI systems could impose risks of a different kind and greater magnitude than seen before, and thus a court could, in principle, treat the development or release of such models as abnormally dangerous or ultrahazardous.[37,42,46] For instance, strict liability could and may apply to fully autonomous vehicles.[42] In practice, however, whether or not courts will actually apply strict liability to AI is extremely unclear.[37,42] Courts are hesitant to expand the set of activities subject to strict liability: they rarely impose strict liability on sellers or distributors rather than owners or possessors (channeling most claims into product liability), and they consider net societal value, which for AI is usually high, meaning it is unlikely to be subject to strict liability.[37,42] However, a developer could face strict liability if a powerful model escapes the developer's possession and causes widespread, catastrophic harm, even after sale or distribution.[37] Overall, there is very little precedent currently applying strict

liability to AI, so any use of this doctrine is likely to be limited and highly specific to the case.[37,42]

1.3.2. European Union's Product Liability Directive:

In the European Union, the doctrine outlining Tort Liability laws is the Product Liability Directive of 1985 (PLD), which imposes no-fault liability on the producer when a defective product causes death, personal injury, or qualifying property damage.[39,41,47] The Directive defines "producer" broadly to include the manufacturer of a finished product, the manufacturer of any component, a producer of raw materials, any person who presents itself as the product's producer, or the importer of an imported product.[41] Moreover, multiple producers can be jointly and severally liable, which is the case for many technology products.[41,47] A product is deemed "defective" if it fails to provide the safety a person is entitled reasonably to expect, assessed in light of the product's presentation (including advertising), its reasonably expected use, and the time it was put into circulation.[41,47] With the emergence of AI, many important definitions in the PLD were directly challenged. For instance, debates emerged over whether AI systems were "products" at all, since many of these systems functioned as services or hybrids, pushing harms caused by AI outside the PLD's scope.[41] In response, a revision to the PLD was proposed and passed to try to account for the new challenges posed by AI.[39,40] The revision answers these challenges by explicitly including software within the definition of a "product," specifically recognizing AI systems as products for the PLD's purposes, and treating AI system providers as manufacturers.[40] It also redefines "component," broadening the definition's scope to include any AI service that is within or related to a product.[40] Moreover, the revision addressed defectiveness in AI contexts, with judges now considering factors specifically tailored to digital systems.[40,47] These factors include the quality of instructions for installation, use, and maintenance; the effect of any ability of continued learning after deployment; the effect of other products reasonably expected to be used alongside it; compliance with safety requirements, including cybersecurity; and the specific expectations of intended users. Lastly, because AI systems are usually complex and opaque, it is often difficult for a victim to provide evidence of a defect and evidence that the defect caused the harms experienced.[39,40,47] To address this burden-of-proof asymmetry, two mechanisms were added: courts may order the disclosure of relevant evidence by the provider, and in certain circumstances, the claim that the AI is defective will be held as true, unless the provider could prove otherwise.[39,40,47] Finally, because AI products are data-dependent, continuously updated, and open-ended, providers could argue that malfunctions stemmed from defective information that influenced the AI after the initial sale. However, the revision addresses this defense: if a manufacturer still had control when defectiveness from services or updates occurred, the original manufacturer is held liable.[40]

1.4. Intermediary Liability:

Intermediary-liability rules distinguish the party that states a message from the platform that it is stated on, protecting the latter.[48] These rules were embedded in early technology policy and enabled both search engines and social media platforms to grow by shielding them from liability for potentially unlawful content posted by third-party users on their platforms.[48] However, the growth of generative AI systems has complicated these rules because generative AI produces new content in accordance with the provider's training rather than solely relaying third-party content.[49,50] As a result, there are ongoing debates about whether and how intermediary-liability frameworks apply to generative AI models. In this section, I examine two very influential frameworks at the core of these debates: Section 230 of the U.S. Communications Decency Act and the European Union's Digital Services Act.

1.4.1. Section 230 of the U.S. Communications Decency Act:

Congress adopted Section 230 in 1996 to promote a competitive online marketplace by protecting online platforms from publisher liability for content supplied by third parties.[11,51] The statute defines an "interactive computer service" (i.e., any platform that enables multiple users to access a computer server), and specifies that such a service may not be treated as the publisher or speaker of information provided by a third-party "information content provider."[49,51] On a literal interpretation, this statute could extend to generative-AI systems, which deliver online information services, accept user prompts, and return responses that might be characterized as pure transformations of user input.[11] In principle, the argument therefore could be made that the safe harbor could apply whenever an output remains sufficiently tied to the user's prompt rather than to independent creative decisions by the model. In practice, however, courts do not apply Section 230 immunity when a service creates or develops the disputed content, even in part. For example, in the cases of *Roommates.com* and Accusearch, the Ninth and Tenth Circuits ruled that even without modifying third-party content, services that contributed partially to its "development" (i.e. adding to or shaping the part of the content that gave rise to the legal claim), are considered "information content providor(s)" rather than neutral intermediaries and therefore were not entitled to Section 230 immunity.[11] This scope includes generative AI systems, since generative AI creates original text rather than merely transmitting third-party speech.[51-53] In addition, generative AI often hallucinates, generating confident but false assertions that do not originate from any third-party speaker, making the provider look less like a conduit and more like a content creator.[11,49-52] Even if it were technically possible to constrain output to be only verbatim quotes from training data, the process of generating output based on probabilities is still distinct from transmitting user-generated content.[54] Moreover, while quotes-only models may technically resemble search functions, most systems still synthesize or edit content in ways that go beyond what a neutral intermediary that simply hosts third-party content would do.[49]

1.4.2. European Union's Digital Services Act:

The applicability of the European Union's Digital Services Act (DSA) is similar to Section 230, in that generative AI is

DOI: 10.36838/IJHSR811.228

not an intermediary; however, the DSA is more complex and contains other regulations that can still apply to generative AI systems. The European Union adopted the DSA in 2022, providing a comprehensive framework for many types of online services that host user-generated content, aiming to tackle illegal content and protect user rights.[55] Similar to Section 230, the DSA sought to promote the growth and innovation of intermediary digital services (i.e., "mere conduit," "hosting," or "caching" services) by shielding them from legal liability for third-party content posted on their platforms.[50,55,56] In this aspect, generative-AI systems do not qualify because their content is produced by the model itself (Arcila, 2023; Novelli *et al.*, 2024).[50,56] However, unlike Section 230, the DSA goes beyond shielding intermediaries, setting responsibilities for online services that aim to strengthen user protections.[50,55,56] If a generative-AI service is used to search the internet, it can reasonably be treated as a search engine, and thus an intermediary, within the DSA framework.[50] In practice, this classification process is case-by-case, relying on how the product functions and is offered to users.[56] For example, if generative AI is embedded in a search engine service, the host service's DSA obligations apply to the embedded service as well.[56] This is the case for Bing Chat, which is integrated in Bing's search engine system and can therefore be treated either as part of the search engine, thus falling under the same regulations that Bing would fall under.[56] For these generative-AI-related search engines, once they are designated a "very large online search engine" (i.e., approximately 45 million monthly active users in the EU), they are required to conduct risk assessments annually and before launching new "high-impact" features.[55] These assessments are extremely comprehensive, covering a plethora of risks arising from the design and use of the embedded generative tool, such as the potential spread of illegal content, effects on natural rights, impacts on minors, and risks to democracy.[50,55,56] The provider must then implement effective mitigations (such as model adjustments, risk disclosures, and watermarking), undergo annual audits, and grant regulators access to data needed to evaluate both risks and mitigations.[50,55,56]

2. Emerging Global Frameworks for Generative AI:

In addition to legacy doctrines, emerging global regulatory frameworks and environments have been developed to address the unique challenges of generative AI, reflecting the growing global consensus that legacy doctrines alone are no longer sufficient to manage generative AI.[13,15] While these frameworks vary in scope and design, they share a common goal of balancing innovation with the protection of individual rights, safety, and security.[17] This section reviews the literature on emerging approaches to AI governance, focusing on the three most prominent regulatory environments, the United States, the European Union, and China, while also examining other influential frameworks that illustrate the diversity of global regulatory responses.

2.1. EU's AI Act:

The EU AI Act is the first comprehensive statute for AI in Europe, adopted to harmonize national regulation, safeguard fundamental rights and safety, and give developers a single set of binding obligations to follow.[13,15,16,57] The EU adopted a rights-based approach, with most duties falling on upstream providers that place systems on the market, while downstream users generally face lighter obligations unless they substantially modify a system, such as fine-tuning, in which case they can be treated as a new provider.[13,15,16,57] The scope of the act is deliberately broad, applying to AI systems in EU markets and to models whose outputs are used in the EU, giving the act practically global reach.[13,16,57] Structurally, the act organizes regulations by four levels of risk: unacceptable risk, high risk, limited risk, and minimal risk.[13,16,57] A narrow set of uses is banned outright if they are deemed an unacceptable risk because they threaten rights or safety, such as systems that assign people a government score to decide access to public services or algorithms that are used to manipulate and exploit vulnerabilities of individuals.[15,57] High-risk AI systems are highly regulated; however, they are not deemed so dangerous that they should be banned, such as in education, migration, employment, or law enforcement.[15,57] Limited-risk (e.g., chatbots or video generation) and Minimal-risk (e.g., video games or email-sending) systems face much lighter rules, such as informing people when they interact with AI or when content is artificially generated.[15,57] Regardless of risk level, however, any developer or provider of AI must comply with Article 4, which requires all staff and agents interacting with an AI system to have adequate AI literacy (i.e., understanding the technicalities, limitations, and regulations of AI).[13] Under the EU Act, there are specific regulations for general-purpose and generative models.[13,15,57] In accordance with Article 53, developers of general-purpose systems must give core technical information on performance, training data, and energy usage to a European regulator, the AI office within the European Commission and any downstream professional users that implement the AI system.[13] Article 53 also extends existing laws regarding data collection and copyright discussed in the previous sections onto AI systems, such as the Text and Data Mining provisions, requiring any developer whose system is used in the EU, regardless if it was trained outside the EU, to comply with these laws and requiring a detailed disclosure of training data sources.[13] Particularly powerful general-purpose systems, or systems deemed to have "systemic risk" face more oversight under Article 55 and Article 14 which require including standardized safety tests, incident reporting, appropriate cybersecurity, as well as requiring a qualified natural person to oversee the development and usage of the high-risk system.[13,57] Lastly, after the system reaches the market providers are required to create a post-market monitoring system to track user interactions and must inform the relevant Market Surveillance Authority for their country within 15 days of any malfunction.[57]

2.2. The United States Regulatory Landscape & AI Action Plan:

The United States recently passed the AI Action Plan under the Trump administration, which guides the U.S. regulatory landscape, aiming to remove regulatory barriers and reduce fragmentation, and setting three priorities: accelerating innova-

tion, building AI infrastructure, and leading internationally.[58,59] However, before reviewing the literature surrounding the AI Action Plan, it is important to first understand the current complex regulatory landscape of the U.S. for AI. Rather than a single set of binding obligations across all industries, such as the EU's AI Act, the U.S. governs AI through a decentralized, market-driven, sector-specific system.[13,60,61] However, the regulatory landscape of the United States does align with many of the principles from international initiatives such as the G7 Hiroshima Process and OECD AI Principles.[60] Moreover, unlike the EU's rights-driven approach and China's state-run model, the U.S. prioritizes innovation and development the most, minimizing state intervention and relying on existing laws, agencies, and voluntary standards.[60,61] While there have been several national policies regarding AI, such as former president Biden's Executive Order on Safe, Secure, and Trustworthy AI, which directed agencies to set safety guardrails for the development and use of AI in their respective sectors, the primary function of most federal policies has been to organize federal practice and standards, avoiding a single cross-sector framework for all private actors.[13,60] Bills that would impose cross-sector duties have been proposed but not yet enacted (e.g., the Algorithmic Accountability Act, which, if passed, would require impact assessments and disclosures to improve transparency and address bias).[60] Thus, the majority of federal regulations affecting AI result from applying existing laws within each domain. For example, the FTC has pursued unfair or deceptive AI practices and moved against AI-enabled impersonation, while the Equal Employment Opportunity Commission has pursued initiatives that enforce equality in employment decisions made by AI.[60] The U.S. also utilizes self-regulatory approaches, including voluntary commitments from major AI developers and frameworks such as NIST's AI Risk Management Framework, a nonbinding framework that provides developers with a comprehensive guide for creating and managing responsible AI systems.[60] Taken together, these elements create a vertical federal layer in which the sector regulator that already oversees important industries like healthcare, finance, transportation, or communications addresses AI uses in that domain, rather than a single horizontal authority. Historically, however, federal action has been slow due to a lack of congressional consensus, resulting in significant regulatory action by state legislatures.[62] In 2024, states proposed 700 AI-related bills, but only a fraction were enacted and, of those, most were conventional or narrow measures such as deepfake protections or the creation of state committees to study AI.[59,62] Notable exceptions to this trend were an AI-transparency bill in California that requires the disclosure of training data, and a civil-rights-based bill in Colorado that protects consumers from algorithmic discrimination.[59] This state-led landscape does have notable advantages. Regulation often responds faster than federal lawmaking, can adapt to emerging use cases, and allows for tailoring to the local priorities of each state.[62] However, at the same time, divergent statutes could create a regulatory patchwork that can increase compliance costs for firms or result in certain states passing overly burdensome regulations, potentially hurting innovation and development.[59,62] This fragmentation and the concern about hurting innovation are among the main incentives for the recent "AI Action Plan" announced by the Trump administration.[58,62,63] To achieve the aforementioned goals delineated by the AI Action Plan, federal agencies will consider a state's "AI regulatory climate" when awarding AI-related funds, examining whether state AI rules conflict with the national priorities.[58,59] These measures are purely advisory, as they guide states through funding choices but do not override any state laws.[63] If the U.S. wanted to truly enforce the priorities of the plan, it would need to pursue broad preemption, which would require Congress or clear delegated authority, but courts generally presume against preemption.[62] Both the level of enforcement and effectiveness of the AI Action Plan are extremely uncertain as details for implementation are vague due to a lack of timelines, lead agencies, or budgeting.[63] However, from this plan, the U.S. has made it clear that its priority is to accelerate AI innovation and maintain global leadership, even if that means loosening domestic guardrails (e.g., supporting broad 'fair use' claims for training data).

2.3. China:

China has one of the world's most developed AI regulatory systems, regulating AI through a sector-specific and state-driven system.[64-66] Its regulatory landscape consists of many different laws and government agencies enforcing them for their respective sector.[64-66] This section will go over the main policies passed over the years, both nationwide and application-specific, as well as explaining how China enforces these laws. The foundation of the regulatory landscape is the New Generation AI Development Plan passed in 2017, which sets a three-phase roadmap until 2030 for AI development and global leadership, while also appointing "national champions" (i.e. specific companies tasked to lead the development of AI in their industry), such as Baidu for autonomous driving, Alibaba for smart cities, and Tencent for medical AI.[64-66] In 2021, China passed the Algorithmic Recommendation Provisions, which introduced the world's first algorithm registry that required companies to disclose information about each algorithm used in their services.[65,66] For example, a single application might have to disclose information for its AI personalized recommendation algorithm and for its AI content filtration algorithm. In 2022, the Provisions on the Administration of Deep Synthesis Internet Information Services were passed, mandating that AI-generated images and videos must be labeled and requiring companies that offer deepfake tools to register algorithms and provide security assessments on their systems.[63,64] In addition to these provisions, to regulate systems that are accessible to the general public, such as chatbots, text-to-image tools for the public, and video generators, China passed the Interim Measures for the Management of Generative AI Services.[65] These measures cover a large portion of AI regulation, mainly updating definitions of existing law and acting as a bridge between legacy doctrines (e.g., IP infringement, data security/collection, and privacy) and AI.[32,65] However, the scope of these measures is restricted to only publicly available systems and excludes systems used privately for research or enterprises.[32,65] These publicly accessible systems must set up a complaint channel

DOI: 10.36838/IJHSR811.228

for users that regulators can use for investigations, undergo a security self-assessment (i.e., disclosing how an algorithm was trained, which datasets it used, what functions it performs), and register their algorithms under the Cyberspace Administration of China (CAC).[32,65] The CAC is one of seven ministries or administrations that enforce the laws that regulate AI. Ministries such as the Ministry of Industry and Information Technology, the Ministry of Public Security, and others coordinate enforcement in their respective domains.[65]

2.4. Other Global Actors:

Alongside the developments of complex regulatory environments in the U.S. and EU, other countries have developed very similar, but not as comprehensive, regulatory frameworks for generative AI.[13,60]

2.4.1. United Kingdom:

The U.K. does not have a single AI Act that regulates all industries; instead, under the White Paper's "pro-innovation approach to AI," it governs generative AI through a sector-specific approach guided by 5 principles that heavily align with the OECD's principles of safety, transparency, fairness, accountability, and contestation.[13,16,67] While the core definition of AI remains the same throughout all industries, how that definition gets applied will differ depending on the domain.[16,67] Moreover, the White Paper puts legal responsibility on the people or organizations in the AI supply chain who are actually in the best position to manage the risk.[16,67] For instance, developers of a model may be required to handle risks related to training data, while the company integrating the AI would be held liable for the impact on end users.

2.4.2. India:

India's approach to generative AI focuses on soft law and standards rather than binding regulation.[3,15] For instance, NITI Aayog, India's prominent policy think tank, played a big role in developing the National Strategy for AI, which aims to align AI development to AI's needs in industries such as healthcare, agriculture, and education, as well as releasing the Responsible AI documents of 2021, which provide both ethical and operational guidance.[3,60] Furthermore, the Ministry of Electronics and Information Technology led implementation programs such as "India AI," which aim to promote innovation and guide workforce deployment.[15] This regulatory environment reflects India's strategy of fostering innovation while adopting safeguards that align with the best international standards.[3,15]

2.4.3. Brazil:

Brazil is advancing a comprehensive framework through Bill No. 2,338/2023, which has passed the Senate and awaits review in the Chamber of Deputies, and attempts to balance innovation with individual rights.[13,68] The bill adopts a risk-based approach modeled after the EU's AI Act. It bans "excessive-risk" applications outright and imposes obligations on high-risk systems, including algorithmic impact assessments, required human oversight, and protections against algorithmic discrimination.[13,68] Generative AI is included within the scope, especially when used in consequential settings such as finance or employment.[13,68]

3. Innovation & Adoption:

In addition to regulation, a central question is how regulation affects the innovation and adoption of generative AI. Because these systems are extremely economically significant, as well as potentially dangerous to society, any policy that regulates AI must balance safeguards with incentives to sustain adoption and promote innovation. Thus, this section will analyze the two most prominent regulatory trends shaping AI governance globally: centralized risk-based frameworks and fragmented decentralized approaches. This section will examine how both regulatory systems pose challenges to sustained innovation despite their differences. Centralized, risk-based regulatory frameworks impose substantial direct costs on innovation through compliance burdens and restrictive constraints. Under the EU's AI Act, compliance is projected to increase operational overhead by about 17 percent and reduce the productivity gains of AI technologies by nearly 30 percent due to strict data-protection laws, with small and medium enterprises disproportionately affected.[69,70] For high-risk AI systems (e.g., those used in medical devices, credit scoring, or educational assessment), a small business with €10 million in turnover could lose 40 percent of its profits due to the EU AI Act.[69] Across the EU, these compliance burdens are projected to reduce AI investments by almost 20 percent.[69] This can also be seen in the United States, where more stringent, risk-based AI regulation (e.g., Colorado's) could reduce the probability of startup fundraising by 2-3 percent annually.[71] This trend of stringent regulation hurting innovation and adoption is not isolated to the EU and U.S. When China allowed AI firms access to government "data-rich" contracts (effectively the opposite of restricting data access through privacy regulation), they were able to build about 20 percent more commercial products and nearly 50 percent more government-facing products within 3 years.[72] Overall, this regulatory environment has constrained European AI development. Over the past two decades, the European Union has produced only three notable AI models compared to the United States' forty and China's fifteen notable models.[73] On adoption, European organizations lag behind their U.S. counterparts by 45 to 70 percent in both AI spending and implementation of technologies.[74]

However, the issue of compliance is not solved in the fragmented system of the US. States have proposed over 700 AI-related bills, and the differing requirements can create substantial complexity for firms operating nationally.[59,62] For example, the varying state privacy laws could impose $98-112 billion annually in out-of-state compliance costs.[75] Colorado's AI Act alone imposes penalties up to $20,000 per violation, exemplifying the escalating compliance burden.[76] For example, a firm adopting AI would have to comply with conflicting standards (e.g., California's data transparency requirements, New York's bias audit mandates, and Colorado's algorithmic discrimination protections) simultaneously.[77] Overall, these compliance costs disproportionately burden smaller firms lacking resources, with one-quarter of small businesses not using

AI citing concerns relating to compliance costs as the main reason for not adopting AI.[76] In this light, the approach of overarching regulation could provide mechanisms that support innovation, as the harmonization of standards under the AI Act and Brazil's Bill 2,338/2023 reduces the negative effects that the U.S. patchwork of state and sector regulations results in, streamlining processes by reducing compliance uncertainty.[17,78] This would be highly beneficial to innovation, as compliance uncertainty is often seen as one of the primary barriers to innovation, especially to smaller firms, as it results in them devoting a higher cost to trying to figure out the convoluted regulations of multiple states or sectors.[78] Ultimately, due to the robust nature of generative AI, it is difficult to attribute the discrepancies between the EU's and the US's AI development solely to regulatory choices. In this section, we have analyzed two prominent regulatory environments and their effects on innovation. Clearly, many countries are trending toward one of two options: either fragmented decentralized regulation or an overarching risk-based framework. While the choice of regulatory approach influences adoption and innovation, factors such as a culture more open to risk-taking (on the entrepreneurial and investor side), greater access to diverse global talent, and the advantage of a large unified home market play an equally or more important role in shaping innovation and adoption.[79]

Conclusion

This paper has examined the governance of generative AI through legacy doctrines, national regulatory environments, and the effect of regulation on innovation. Within legacy doctrines, comparative analysis was essential to identify three fundamental challenges that persist: (1) protecting privacy in the training and outcomes of AI systems, (2) determining whether AI can or should be treated as a legal or creative entity capable of holding rights or responsibilities, and (3) addressing how the autonomy of AI systems complicates the attribution of intention and decision-making in areas such as authorship and liability. Across all three challenges, it is increasingly evident that current frameworks being applied are not up to date on the technical challenges of AI, such as the persistence of data in model parameters and the opacity of the decision-making process of AI systems. While some existing frameworks have been updated or revised to address AI directly (e.g., the EU's reform of the Product Liability Directive), in most cases, adoption has been left to courts to decide on a case-by-case basis, such as the U.S. fair use disputes in copyright, resulting in an inconsistent and inadequate response to an ever-growing challenge.[37,40]

Countries have also begun to develop national frameworks and regulatory environments to specifically address the new challenges posed by AI.[13,15] These emerging national regulations fall into four main approaches: (1) risk-based approach, such as the EU AI Act and Brazil's Bill 2,338/2023; (2) innovation-first systems, such as in the U.S. which rely on sectoral agencies; (3) state-directed systems like China's regulatory environment; (4) and voluntary or soft-law approaches in India and the U.K., which emphasize guidelines over binding rules. Although these approaches share common elements, such as prohibiting unacceptable uses, requiring some level of transparency, and trying to protect individual rights, through comparative analysis, it is evident that the regulation of AI is too fragmented. Attempting to harmonize the approaches reviewed in this paper would be highly beneficial, as harmonization could provide global consistency, establish universal ethical standards, address transnational challenges, and allow for enhanced public trust and global cooperation.[17] Nevertheless, this study has limitations. Its reliance on comparative legal analysis constrains its ability to evaluate the real-world impact of these frameworks on innovation. Moreover, the relative novelty of generative AI means that robust empirical data remains limited, making it difficult to measure how specific regulatory approaches affect innovation, startup formation, and investment. Future research should therefore focus on developing empirical methods to assess these impacts and explore how regulation can ensure accountability and protection of human rights without impeding technological progress.

Acknowledgments

I'd like to acknowledge Plinio Zanini and Dr. Siddharth Krishnan, as well as Indigo Research, for their invaluable guidance and support throughout the development of this paper. I attest that the ideas, graphics, and writing in this paper are entirely my own.

References

1. Takale, D.; Mahalle, P.; Sule, B. (PDF) Advancements and Applications of Generative Artificial Intelligence. *J. Inf. Technol. Sci.* **2024**, *10* (1).
2. Chui, M.; Hazan, E.; Roberts, R.; Singla, A.; Smaje, K.; Sukharevsky, A.; Yee, L.; Zemmel, R. The Economic Potential of Generative AI. The next Productivity Frontier. **2023**.
3. Joshi, S. Generative AI: Mitigating Workforce and Economic Disruptions While Strategizing Policy Responses for Governments and Companies. Social Science Research Network: Rochester, NY, February 12, 2025. https://doi.org/10.2139/ssrn.5135229.
4. Salari, N.; Beiromvand, M.; Hosseinian-Far, A.; Habibi, J.; Babajani, F.; Mohammadi, M. Impacts of Generative Artificial Intelligence on the Future of the Labor Market: A Systematic Review. *Comput. Hum. Behav. Rep*. **2025**, *18*, 100652. https://doi.org/10.1016/j.chbr.2025.100652.
5. Oder, N.; Béland, D. Artificial Intelligence, Emotional Labor, and the Quest for Sociological and Political Imagination among Low-Skilled Workers. *Policy Soc.* **2025**, *44* (1), 116–128. https://doi.org/10.1093/polsoc/puae034.
6. Babaei, R.; Cheng, S.; Duan, R.; Zhao, S. Generative Artificial Intelligence and the Evolving Challenge of Deepfake Detection: A Systematic Analysis. *J. Sens. Actuator Netw*. **2025**, *14* (1), 17. https://doi.org/10.3390/jsan14010017.
7. Chesterman, S. Good Models Borrow, Great Models Steal: Intellectual Property Rights and Generative AI. *Policy Soc*. **2024**, *44* (1), 23–37. https://doi.org/10.1093/polsoc/puae006.
8. Jaidka, K.; Chen, T.; Chesterman, S.; Hsu, W. *Misinformation, Disinformation, and Generative AI: Implications for Perception and Policy | Digital Government: Research and Practice*. https://dl.acm.org/doi/10.1145/3689372 (accessed 2025-07-30).

DOI: 10.36838/IJHSR811.228

9. Judge, B.; Nitzberg, M.; Russell, S. When Code Isn't Law: Rethinking Regulation for Artificial Intelligence. *Policy Soc*. **2025**, *44* (1), 85–97. https://doi.org/10.1093/polsoc/puae020.
10. Zaidan, E.; Ibrahim, I. A. AI Governance in a Complex and Rapidly Changing Regulatory Landscape: A Global Perspective. *Humanit. Soc. Sci. Commun*. **2024**, 11 (1), 1121. https://doi.org/10.1057/s41599-024-03560-x.
11. Ryan, G. Generative AI Will Break the Internet: Beyond Section 230. Social Science Research Network: Rochester, NY, May 10, 2024. https://doi.org/10.2139/ssrn.5337202.
12. Buiten, M.; de Streel, A.; Peitz, M. The Law and Economics of AI Liability. *Comput. Law Secur. Rev*. **2023**, *48*, 105794. https://doi.org/10.1016/j.clsr.2023.105794.
13. Hacker, P.; Engel, A.; Hammer, S.; Mittelstadt, B. Introduction to the Foundations and Regulation of Generative AI. Social Science Research Network: Rochester, NY, February 14, 2025. https://doi.org/10.2139/ssrn.5137750.
14. Atkinson, D.; Morrison, J. A Legal Risk Taxonomy for Generative Artificial Intelligence. arXiv May 23, 2024. https://doi.org/10.48550/arXiv.2404.09479.
15. Davtyan, T. An Overview of Global Efforts Towards AI Regulation. *Bull. Yerevan Univ. C Jurisprud*. **2024**, *15* (2 (41)), 158–174. https://doi.org/10.46991/BYSU.C/2024.15.2.158.
16. Cole, M. *AI Regulation and Governance on a Global Scale: An Overview of International, Regional and National Instruments*. https://doi.org/10.21552/aire/2024/1/16.
17. Kashefi, P.; Kashefi, Y.; Ghafouri Mirsaraei, A. Shaping the Future of AI: Balancing Innovation and Ethics in Global Regulation. *Unif. Law Rev*. **2024**, *29* (3), 524–548. https://doi.org/10.1093/ulr/unae040.
18. Raza, S.; Qureshi, R.; Zahid, A.; Fioresi, J.; Sadak, F.; Saeed, M.; Sapkota, R.; Jain, A.; Zafar, A.; Hassan, M. U.; Zafar, A.; Maqbool, H.; Vayani, A.; Wu, J.; Shoman, M. Who Is Responsible? The Data, Models, Users, or Regulations? A Comprehensive Survey on Responsible Generative AI for a Sustainable Future. arXiv April 28, 2025. https://doi.org/10.48550/arXiv.2502.08650.
19. Taeihagh, A. Governance of Generative AI. *Policy Soc*. **2025**, *44* (1), 1–22. https://doi.org/10.1093/polsoc/puaf001.
20. Janssen, M. Responsible Governance of Generative AI: Conceptualizing GenAI as Complex Adaptive Systems. *Policy Soc*. **2025**, *44* (1), 38–51. https://doi.org/10.1093/polsoc/puae040.
21. Luna, J.; Tan, I.; Xie, X.; Jiang, L. Navigating Governance Paradigms: A Cross-Regional Comparative Study of Generative AI Governance Processes & Principles. Proc. AAAIACM Conf. *AI Ethics Soc*. **2024**, *7* (1), 917–931. https://doi.org/10.1609/aies.v7i1.31692.
22. King, J.; Meinhardt, C. *Rethinking Privacy in the AI Era: Policy Provocations for a Data-Centric World | Stanford HAI*. https://hai.stanford.edu/policy/white-paper-rethinking-privacy-ai-era-policy-provocations-data-centric-world (accessed 2025-09-04).
23. Ruschemeier, H. Generative AI and Data Protection. *Camb. Forum AI Law Gov*. **2025**, *1*, e6. https://doi.org/10.1017/cfl.2024.2.
24. de Jonge, A. Data Privacy in China and Europe: Individual, Collective, Subjective, and Objective Perspectives. *Int. J. Law Inf. Technol*. **2024**, *32*, eaae025. https://doi.org/10.1093/ijlit/eaae025.
25. Ye, X.; Yan, Y.; Li, J.; Jiang, B. Privacy and Personal Data Risk Governance for Generative Artificial Intelligence: A Chinese Perspective. *Telecommun. Policy* **2024**, *48* (10), 102851. https://doi.org/10.1016/j.telpol.2024.102851.
26. Arokun, E. Complexities of AI Trends: Threats to Data Privacy Legal Compliance. Social Science Research Network: Rochester, NY, May 6, 2024. https://doi.org/10.2139/ssrn.4943466.
27. Haile, A.; Ashraf, M. *(PDF) Data Protection and AI: Navigating Regulatory Compliance in AI- Driven Systems*. ResearchGate. https://doi.org/10.13140/RG.2.2.13639.92328.
28. Qiu, Y.; Yu, H.; Fang, H.; Zhuang, T.; Yu, W.; Chen, B.; Wang, X.; Xia, S.-T.; Xu, K. MIBench: A Comprehensive Framework for Benchmarking Model Inversion Attack and Defense. arXiv March 10, 2025. https://doi.org/10.48550/arXiv.2410.05159.
29. Calzada, I. Citizens' Data Privacy in China: The State of the Art of the Personal Information Protection Law (PIPL). Social Science Research Network: Rochester, N, Y September 8, 2022. https://papers.ssrn.com/abstract=4214011 (accessed 2025-09-04).
30. Shao, G.; Huang, Q.; Xiang, Q.; Peng, C. Assessing the Implementation of China's Personal Information Protection Law: A Two-Year Review. *Int. Data Priv. Law* **2025**, *15* (1), 18–31. https://doi.org/10.1093/idpl/ipae022.
31. Gao, R. Y. Personal Information Protection Under Chinese Civil Code: A Newly Established Private Right in the Digital Era. Social Science Research Network: Rochester, NY 2020. https://papers.ssrn.com/abstract=3934721 (accessed 2025-09-04).
32. Zou, M.; Zhang, L. Navigating China's Regulatory Approach to Generative Artificial Intelligence and Large Language Models. Camb. *Forum AI Law Gov*. **2025**, *1*, e8. https://doi.org/10.1017/cfl.2024.4.
33. Poland, C. M. Generative AI and US Intellectual Property Law. arXiv November 27, 2023. https://doi.org/10.48550/arXiv.2311.16023.
34. Okoro, D. C. An Intellectual Property Approach to the Use of Generative AI. *World J. Innov. Mod. Technol*. **2025**, *9* (4), 97–116.
35. Oladele, O. K. *(PDF) Generative AI and Intellectual Property: Ownership, Copyright, and Creative Rights*. ResearchGate. https://www.researchgate.net/publication/390033354_Generative_AI_and_Intellectual_Property_Ownership_Copyright_and_Creative_Rights (accessed 2025-09-04).
36. Mammen, C.; Collyer, M.; Dolin, R. A.; Gangjee, D. S.; Melham, T.; Mustaklem, M.; Sundaralingam, P.; Wang, V. Creativity, Artificial Intelligence, and the Requirement of Human Authors and Inventors in Copyright and Patent Law. Social Science Research Network: Rochester, NY, July 5, 2024. https://doi.org/10.2139/ssrn.4892973.
37. Ramakrishnan, K.; Smith, G.; Downey, C. *U.S. Tort Liability for Large-Scale Artificial Intelligence Damages: A Primer for Developers and Policymakers*; 2024. https://www.rand.org/pubs/research_reports/RRA3084-1.html (accessed 2025-08-27).
38. Lior, A. *Holding AI Accountable: Addressing AI-Related Harms Through Existing Tort Doctrines | The University of Chicago Law Review*. https://lawreview.uchicago.edu/online-archive/holding-ai-accountable-addressing-ai-related-harms-through-existing-tort-doctrines (accessed 2025-08-27).
39. Noto La Diega, G.; Bezerra, L. C. T. Can There Be Responsible AI without AI Liability? Incentivizing Generative AI Safety through Ex-Post Tort Liability under the EU AI Liability Directive. *Int. J. Law Inf. Technol*. **2024**, *32*, eaae021. https://doi.org/10.1093/ijlit/eaae021.
40. Rodríguez de las Heras Ballell, T. The Revision of the Product Liability Directive: A Key Piece in the Artificial Intelligence Liability Puzzle. *ERA Forum* **2023**, *24* (2), 247–259. https://doi.org/10.1007/s12027-023-00751-y.
41. Cabral, T. S. Liability and Artificial Intelligence in the EU: Assessing the Adequacy of the Current Product Liability Directive. *Maastricht J. Eur. Comp. Law* **2020**, *27* (5), 615–635. https://doi.org/10.1177/1023263X20948689.

42. Herbosch, M. Liability for AI Agents. Social Science Research Network: Rochester, NY April 28, 2025. https://doi.org/10.2139/ssrn.5236649.
43. Selbst, A. D. Negligence and AI's Human Users. Social Science Research Network: Rochester, NY, March 11, 2019. https://papers.ssrn.com/abstract=3350508 (accessed 2025-09-04).
44. Fraser, H. L.; Suzor, N. Locating Fault for AI Harms: A Systems Theory of Foreseeability, Reasonable Care and Causal Responsibility in the AI Value Chain. Social Science Research Network: Rochester, NY April 26, 2024. https://doi.org/10.2139/ssrn.5190797.
45. Chagal-Feferkorn, K. Am I an Algorithm or a Product? When Products Liability Should Apply to Algorithmic Decision-Makers. Social Science Research Network: Rochester, NY August 14, 2018. https://papers.ssrn.com/abstract=3241200 (accessed 2025-09-04).
46. Henson, R. "I Am Become Death, the Destroyer of Worlds": Applying Strict Liability to Artificial Intelligence as an Abnormally Dangerous Activity. Social Science Research Network: Rochester, N, Y July 15, 2024. https://doi.org/10.2139/ssrn.4894986.
47. Karanikić Mirić, M. Product Liability Reform in the EU. Social Science Research Network: Rochester, NY, November 7, 2023. https://papers.ssrn.com/abstract=4626103 (accessed 2025-09-04).
48. Grimmelmann, J.; Zhang, P. An Economic Model of Intermediary Liability. Social Science Research Network: Rochester, NY April 19, 2023. https://papers.ssrn.com/abstract=4422819 (accessed 2025-08-11).
49. Lemley, M. A.; Henderson, P.; Hashimoto, T. Where's the Liability in Harmful AI Speech? Social Science Research Network: Rochester, NY, August 3, 2023. https://doi.org/10.2139/ssrn.4531029.
50. Arcila, B. Is It a Platform? Is It a Search Engine? It's Chat GPT! The European Liability Regime for Large Language Models. Social Science Research Network: Rochester, NY August 12, 2023. https://papers.ssrn.com/abstract=4539452 (accessed 2025-08-12).
51. Ariyaratne, H. ChatGPT and Intermediary Liability: Why Section 230 Does Not and Should Not Protect Generative Algorithms. Social Science Research Network: Rochester, NY, May 16, 2023. https://doi.org/10.2139/ssrn.4422583.
52. Volokh, E. Large Libel Models? Liability for AI Output. Social Science Research Network: Rochester, NY August 19, 2023. https://papers.ssrn.com/abstract=4546063. (accessed 2025-08-11).
53. Davidson, J.; Buttrick, H. *(PDF) SAY WHAT?! When ChatGPT Gets it Wrong: EXAMINING GENERATIVE AI, SECTION 230 OF THE COMMUNICATIONS DECENCY ACT, AND THE ESSENCE OF CREATIVITY*. ResearchGate. https://www.researchgate.net/publication/376953148_SAY_WHAT_When_ChatGPT_Gets_it_Wrong_EXAMINING_GENERATIVE_AI_SECTION_230_OF_THE_COMMUNICATIONS_DECENCY_ACT_AND_THE_ESSENCE_OF_CREATIVITY (accessed 2025-09-04).
54. Cheong, I.; Caliskan, A.; Kohno, T. Safeguarding Human Values: Rethinking US Law for Generative AI's Societal Impacts. *AI Ethics* **2025**, *5* (2), 1433–1459. https://doi.org/10.1007/s43681-024-00451-4.
55. Wilman, F. The Digital Services Act (DSA) - An Overview. Social Science Research Network: Rochester, NY December 16, 2022. https://doi.org/10.2139/ssrn.4304586.
56. Novelli, C.; Casolari, F.; Hacker, P.; Spedicato, G.; Floridi, L. Generative AI in EU Law: Liability, Privacy, Intellectual Property, and Cybersecurity. Computer Law & Security Review 2024, 55, 106066. https://doi.org/10.1016/j.clsr.2024.106066.
57. Edwards, L. The EU AI Act: A Summary of Its Significance and Scope, 2022. https://www.adalovelaceinstitute.org/wp-content/uploads/2022/04/Expert-explainer-The-EU-AI-Act-11-April-2022.pdf (accessed 2025-09-08).
58. Schildkraut, P.; Curtis, D.; Choi, E.; Magnani, T.; Lee, R.; Annatoyn, T.; Rhea, S.-M.; Magnani, T. *America's AI Action Plan: What Full Steam Ahead Means for Your Company | Advisories.* Arnold & Porter. https://www.arnoldporter.com/en/perspectives/advisories/2025/07/americas-ai-action-plan (accessed 2025-09-06).
59. Ball, D. W. *The Coming Year of AI Regulation in the States | TechPolicy.Press*. Tech Policy Press. https://techpolicy.press/the-coming-year-of-ai-regulation-in-the-states (accessed 2025-09-06).
60. Davtyan, T. The U.S. Approach to AI Regulation: Federal Laws, Policies, and Strategies Explained. *J. Law Technol. Internet* **2025**, *16* (2), 223.
61. Roberts, H.; Cowls, J.; Hine, E.; Mazzi, F.; Tsamados, A.; Taddeo, M.; Floridi, L. Achieving a 'Good AI Society': Comparing the Aims and Progress of the EU and the US. *Sci. Eng. Ethics* **2021**, *27* (6), 68. https://doi.org/10.1007/s11948-021-00340-7.
62. Novelli, C.; Gaur, A.; Floridi, L. Two Futures of AI Regulation under the Trump Administration. Social Science Research Network: Rochester, NY, March 31, 2025. https://doi.org/10.2139/ssrn.5198926.
63. Meinhardt, C.; Zhang, D.; King, J.; Haupt, A.; Cryst, E. *Inside Trump's Ambitious AI Action Plan | Stanford HAI*. https://hai.stanford.edu/news/inside-trumps-ambitious-ai-action-plan (accessed 2025-09-06).
64. Roberts, H.; Cowls, J.; Morley, J.; Taddeo, M.; Wang, V.; Floridi, L. The Chinese Approach to Artificial Intelligence: An Analysis of Policy, Ethics, and Regulation. Social Science Research Network: Rochester, NY, September 1, 2019. https://doi.org/10.2139/ssrn.3469784.
65. Zhang, A. H. The Promise and Perils of China's Regulation of Artificial Intelligence. Social Science Research Network: Rochester, NY January 28, 2024. https://doi.org/10.2139/ssrn.4708676.
66. Sheehan, M. China's AI Regulations and How They Get Made. *Horiz. J. Int. Relat. Sustain. Dev*. **2023**, No. 24, 108–125.
67. Gikay, A. A. Risks, Innovation, and Adaptability in the UK's Incrementalism versus the European Union's Comprehensive Artificial Intelligence Regulation. *Int. J. Law Inf. Technol.* **2024**, *32*, eaae013. https://doi.org/10.1093/ijlit/eaae013.
68. Ziosi, M.; Hwu, R.; Guedes, P.; Freiman, O.; Yeo, H. *A Comparative Framework for AI Regulatory Policy: Phase* 2; 2024. https://ceimia.org/wp-content/uploads/2024/06/a-comparative-framework-for-ai-regulatory-policy_-phase-2-report.pdf.
69. Mueller, B. How Much Will the Artificial Intelligence Act Cost Europe?, 2021. https://www2.datainnovation.org/2021-aia-costs.pdf.
70. Misch, F.; Sher, G.; Park, B.; Pizzinelli, C. *AI and Productivity in Europe*. IMF. https://www.imf.org/en/Publications/WP/Issues/2025/04/04/AI-and-Productivity-in-Europe-565924 (accessed 2025-09-08).
71. Mulla, J. AI Regulation and Entrepreneurship. Social Science Research Network: Rochester, NY, October 11, 2024. https://doi.org/10.2139/ssrn.4986041.
72. Beraja, M.; Yang, D. Y.; Yuchtman, N. Data-Intensive Innovation and the State: Evidence from AI Firms in China. *Rev. Econ. Stud*. **2023**, *90* (4), 1701–1723. https://doi.org/10.1093/restud/rdac056.
73. Maslej, N.; Fattorini, L.; Cortez, E. K.; Lotufo, J. B.; Reuel, A.; Rome, A.; Salatino, A.; Santarlasci, L.; Brynjolfsson, E.; Clark, J.; Etchemendy, J.; Ligett, K.; Lyons, T.; Chase, Jpm.; Manyika, J.; Niebles, J. C.; Parli, V.; Shoham, Y.; Wald, R.; Capstick, E.; Kariuki, N.; Glismann, M. van D.; Hamrah, A.; Oak, S.; Paintsil, N. F.; Shi, A. Artificial Intelligence Index Report 2025 Policy Highlights. Stanford University Human-Centered Artificial Intelligence 2025.

DOI: 10.36838/IJHSR811.228

74. Sukharevsky, A.; Hazan, E.; Smit, S.; Dagorret, G.; Mischke, J.; Hieronimus, S.; de Jong, M.; de la Chevasnerie, M.-A. AI in Europe: A new opportunity for growth | McKinsey. https://www.mckinsey.com/capabilities/quantumblack/our-insights/time-to-place-our-bets-europes-ai-opportunity (accessed 2025-11-07).
75. Castro, D.; Diebold, G.; Dascoli, L. The Looming Cost of a Patchwork of State Privacy Laws; 2022. https://itif.org/publications/2022/01/24/looming-cost-patchwork-state-privacy-laws/ (accessed 2025-11-07).
76. Stevens, M. State of Confusion: How a Patchwork of AI Laws Hurts Small Businesses and U.S. Competitiveness. ACT | The App Association. https://actonline.org/2025/10/10/state-of-confusion-how-a-patchwork-of-ai-laws-hurts-small-businesses-and-u-s-competitiveness/ (accessed 2025-11-07).
77. Shields, T. The AI Regulation Nightmare: Why State-by-State Rules are Crushing Your Business Innovation. Kelley Kronenberg. https://www.kelleykronenberg.com/blog/the-ai-regulation-nightmare-why-state-by-state-rules-are-crushing-your-business-innovation/ (accessed 2025-11-07).
78. Wu, W.; Liu, S. Compliance Costs of AI Technology Commercialization: A Field Deployment Perspective. arXiv January 31, 2023. https://doi.org/10.48550/arXiv.2301.13454.
79. Bradford, A. The False Choice Between Digital Regulation and Innovation. Social Science Research Network: Rochester, NY, March 7, 2024. https://doi.org/10.2139/ssrn.4753107.

Authors

Ryan Chen is a high school senior interested in Law, Economics, and Artificial Intelligence. He is passionate about exploring how policy and technology intersect. In his free time, Ryan enjoys photography and writing.