

A Comparative Study of Deepfake Policy in the United States and China

Xinzhi Wang

Meiji University, Tokyo, Japan

Abstract: *The rapid development of Deepfake technology has brought about innovative applications, but has also raised concerns about privacy, security, and information manipulation. This study compares the deep forgery technology policies of shopping platforms in China and the United States, and analyzes the similarities and differences in regulation between the two countries. Firstly, this paper reviews the existing policy frameworks of the two countries, examines the policy background, legislative basis, regulatory structure, and specific measures, and elaborates on the threat of Deepfake technology to society. Next, it analyzes the public attitude survey data of the two countries to explore the respondents' perception and trust in technology and its regulation, highlighting the differences in policy effectiveness in reality. By using statistical methods to test the difference in public trust between the two countries, it evaluates the social acceptance of policy implementation. Based on the research results, the paper proposes policy optimization suggestions to assist the government in promoting technological innovation, reducing potential risks of Deepfake technology, and providing reference for subsequent policy improvement.*

Keywords: *Deepfake Policy, Technology Governance Framework, Trust Level*

1. Research background

1.1 The rise and application of Deepfake technology

With the booming development of neural networks and deep learning technologies, deep network models have become the main tool for training large-scale image and video datasets to generate highly realistic virtual faces. Deepfake technology uses deep learning technology to synthesize faces. The initial motivation came from providing users with entertainment, auxiliary visual effects, and expanding data sets. However, in recent years, Deepfake technology has been abused by criminals, resulting in many problems such as telecommunications fraud, pornography dissemination, infringement of portrait rights, and manipulation of public opinion. Content creators exploit the hyper-realistic capabilities of deepfake technology to produce deceptive videos, disseminating false narratives to manipulate public sentiment and undermine societal trust. When the public realizes that they cannot discern the authenticity of video content, suspicion and distrust of all information increases, inevitably undermining the broader framework of social trust[1].

1.2 The impact of Deepfake technology on society and politics

1.2.1 Decline in Information Trustworthiness

In modern society, personal security is closely intertwined with information security. When disinformation saturates the information environment, it obscures the truth, distorts public perception, and disrupts decision-making and behavior. Its profound impact extends across economic, political, and cultural spheres, threatening people's lives and property[2]. In other words, deepfake manipulation operates by strategically exploiting public sentiment[1]. When people's lives are filled with manipulative content and strategic deception, uncertainty and insecurity surge sharply, leading to increased reliance on disinformation and a gradual decline in critical thinking abilities.

1.2.2 Safeguarding National Security and Institutional Stability

Deepfake in the post-public sphere operates not merely as distortion but as a strategic tool to erode deliberative democracy. It mobilizes emotionalized collectives and cognitive biases, undermining rational public discourse and destabilizing political legitimacy[1]. In other words, malicious actors

exploit the rapid dissemination characteristics of social media to implant disinformation within the target society, inciting ethnic, religious conflicts, and social unrest, which may escalate into public opinion crises or even political turmoil.

1.2.3 Undermining Democracy and Electoral Integrity

Deepfake is often employed in political campaigns, where the public may manipulate its impact to influence election outcomes or discredit political opponents. Such as ,in some instances, whataboutism can be a deliberate technique to subvert conversations[1]. The practices can erode public trust in the government and even democratic institutions. For instance, individuals may employ "whataboutism" tactics to divert attention from a current issue or political figure by shifting focus to another topic or personality. For example, in 2020, an incident related to the Black Lives Matter movement occurred. Subsequently, certain individuals produced videos through selective editing, collage, and distortion of facts, deliberately portraying the event as violent acts by looters against U.S. law enforcement, thereby framing it as a threat to national security. By disseminating disinformation to instill non-factual narratives and create a false perception of public consensus, this approach suppresses authentic voices and undermines the nation's democratic progress.

1.3 Significance of the study

With the popularization of shopping applications, Deepfake videos have become a new marketing tool, bringing innovation and ethical legal challenges. Studying the policy differences between China and the United States has academic value.

1.4 Research purposes and questions

China and the United States have already noticed the phenomenon of Deepfakes and have formulated a series of laws and policies. Although the two countries have different priorities for policy making, neither country has strict supervision over Deepfakes in shopping apps.

Q1: China/US: Evaluate countries' strategies and effectiveness in educating citizens to identify and resist Deepfakes.

Q2: How to learn from each other and better address the risks posed by Deepfakes.

1.5 Research Scope and Methodology

This study focuses on regulatory approaches to Deepfake technology, systematically examining the feasibility and effectiveness of governance frameworks through policy analysis, empirical data, and cross-national comparative research. The specific methodologies are as follows:

1.5.1 Policy Analysis

Scope: Selected policy documents from the United States and China will be analyzed.

Method: Utilizing policy instrument theory, the study will deconstruct regulatory mechanisms to assess their design logic and potential gaps.

1.5.2 Survey Data Analysis

Data Sources: Public perception surveys on Deepfakes conducted in China and the U.S.

Focus: Quantifying cross-national differences in public risk perception of Deepfakes and evaluating the alignment between regulatory policies and societal demands.

1.5.3 Comparative Analysis

Cross-National Comparison: Contrasting China's proactive content moderation model with the U.S.'s legal-liability approach.

Legislative Dynamics: Examining policy evolution in both countries to identify challenges in regulatory harmonization.

1.6 Conceptual Definitions

"Deepfake video" refers to the use of deep learning, virtual reality and other generative synthesis

algorithms to create videos with virtual scenes and biometric features, including but not limited to (see Figure 1):

- (1) Generate or edit biometric information such as faces, voices, etc.
- (2) Face generation, face replacement, face manipulation, gesture manipulation and other character image and video generation or videos that significantly change personal identity characteristics.
- (3) Three-dimensional reconstruction, digital simulation and other technologies for generating or editing digital characters and virtual scenes.
- (4) In video, any speech, conduct, or depiction which causes, or a reasonable person would recognize has a tendency to cause perceptible individual or societal harm, including misrepresentation, reputational damage, embarrassment, harassment, financial losses, the incitement of violence, the alteration of a public policy debate or election, or the furtherance of any unlawful act.

		DEFINITIONS		Regulatory Authority
China	DOCUMENT	DEFINITIONS		
	Provisions on Ecological Governance of Network Information Content	Article 23 Network information content service users, network information content producers, and network information content service platforms are not allowed to use new technologies and applications such as deep-learning and virtual reality to engage in activities prohibited by laws and administrative regulations.		The Cyberspace Administration of China, CAC
	Provisions on the Administration of Deep Synthesis of Internet-Based Information Service	Article 45 (1) Generate or edit biometric information such as faces, voices, etc.; (2) Generate or edit non-biometric information such as special objects and scenes that may involve national security, national image, national interests and social public interests. Article 47 (1) Intelligent dialogue, intelligent writing and other services that simulate natural persons to generate or edit text; (2) Editing services that generate speech such as synthesized human voices, imitated voices, or significantly change personal identity characteristics; (3) Editing services such as face generation, face replacement, face manipulation, posture manipulation and other character image and video generation or significant changes in personal identity characteristics; (4) Immersive simulation scene generation or editing services; (5) Other services that have the function of generating or significantly changing information content. Article 23 Deep synthesis technology refers to technology that uses generative synthesis algorithms such as deep learning and virtual reality to produce network information such as text, images, audio, video, and virtual scenes.		State Administration of Radio and Television police Department
	National S.2159 - Deepfake Task Force Act S.2159 — 117th Congress (2021-2022)	(1) DIGITAL CONTENT FORGERY.—The term “digital content forgery” means the use of emerging technologies, including artificial intelligence and machine learning techniques, to fabricate or manipulate audio, visual, or text content with the intent to mislead.		National Security Agency, NSA
US	National THE 116TH CONGRESS SESSION H. R. 5186	(1) ADVANCED TECHNOLOGICAL FALSE PERSONATION RECORD.—The term “advanced technological false personation record” means any Deepfake, which—(A) a reasonable person, having considered the visual or audio qualities of the record and the nature of the distribution channel in which the record appears, would believe accurately exhibit— (i) any material activity of a living person which such living person did not in fact undertake; or (ii) any material activity of a deceased person which such deceased person did not in fact undertake; and the exhibition of which is substantially likely to either further a criminal act or result in improper interference in an official proceeding, a public policy debate, or an election; and “(B) was produced without the consent of such living person, or in the case of a deceased person, such person or the heirs thereof.” (3) “The term “Deepfake” means any video recording, motion picture film, sound recording, electronic image, or photograph, or any technological representation of speech or conduct substantially derivative thereof.—”		Federal Trade Commission, FTC
	California Deepfake REPORT ACT OF 2019	This section defines “digital content forgery” as the use of emerging technologies, including artificial intelligence and machine learning techniques, to fabricate or manipulate audio, visual, or text content with the intent to mislead.		Federal Communications Commission, FCC
	Cal Elec. Code § 20010(a) (2020).	“Materially deceptive audio or visual media” mean: 1. Falsely appear to a reasonable person to be authentic; and 2. “Cause a reasonable person to have a fundamentally different understanding or impression of the expressive content” than if he or she had seen the unaltered content. § 20010(e).		Department of Justice, DOJ
	Texas Texas Election Code §215.004	In this section, “Deepfake video” means a video, created with the intent to deceive, that appears to depict a real person performing an action that did not occur in reality.		
	Virginia Code of Virginia § 18.2-386.2.	For purposes of this subsection, “another person” includes a person whose image was used in creating, adapting, or modifying a videographic or still image with the intent to depict an actual person and who is recognizable as an actual person by the person’s face, likeness, or other distinguishing characteristic.		

Figure 1 Definitions of Deepfake in China and the United States

2. Technical background

2.1 Introduction to Deepfake technology

From the perspective of technological evolution and innovation theory, Deepfake technology is essentially the result of disruptive innovation. In the 1940s, economist Joseph A. Schumpeter proposed the theory of creative destruction, pointing out that innovation is the endogenous driving force of economic growth, including new technologies, new products, new markets and other factors. The technological revolution is the key driver of innovation. Clayton M. Christensen said that technological innovation can be divided into continuous innovation and disruptive innovation.

In the field of artificial intelligence, the emergence of "Deepfakes" is a typical example of the transition of deep learning technology from continuous innovation to disruptive innovation. Deep forgery technology uses GAN architecture, where the generator generates data and the discriminator identifies authenticity to improve performance in adversarial situations.

2.2 Development history of Deepfake technology

2.2.1 The evolution of Deepfake technology

Since George Washington Wilson's fake group photo in 1857, photo manipulation techniques have continued to develop. In 1860, the first manipulated photograph was released. With the emergence of tools such as Photoshop, digital retouching technology developed in the late 20th century[3]. In 1997, a video rewriting program used machine learning to achieve facial synchronization, marking a major breakthrough in technology[4]. Entering the 21st century, image editing technology can automate the processing of complex visual effects. In 2016, Deepfake technology was widely used, and in January 2022, GAN technology made significant progress[5].

2.2.2 Application of Deepfake technology in different fields

(1) Positive Effects

In scientific research, deep forgery is used to assist in data training and high-risk experimental simulations, such as using autonomous driving (AADS) to complete tests.. In terms of education, we aim to recreate historical figures and restore damaged or lost cultural relics. In the cultural field, deep forgery enriches the audio-visual effects of film, television, and games to enhance entertainment effects.

In the medical field, Deepfake technology can not only generate digital images that are indistinguishable from medical images for doctors to refer to, but sometimes it can even directly intervene in the treatment and rehabilitation process.

In the social field, Deepfakes can create virtual identities for consumers to participate in various social activities.

(2) Negative effects

Regarding personal privacy, the misuse of Deepfake technology for impersonating others and tampering with copyrighted works such as movies, TV shows, and music has become an increasingly serious problem. The "Liar's Dividend"[6]. As for the overall meaning that people associate with advertising, one of the biggest issues might be that misinformation, disinformation and fake news all contribute to a trend of skepticism toward information truthful or otherwise, and perhaps even a post-truth society[7]. Even if consumers know that they were exposed to fake content, the persuasive effects of that content still have a lasting influence on later perceptions, even when the credibility of content is shown to be questionable or even misleading[8].

2.3 Potential risks and challenges of Deepfake technology

2.3.1 The possibility of false information and privacy leakage

(1) Copyright infringement

Deep forgery techniques often use other people's works to modify data, making it difficult to define the ownership of new works, leading to frequent disputes over individual copyright. Unauthorized dissemination not only deprives the original author of their rights and undermines their motivation, but also disrupts the balance of the creative industry.

(2) Sexual privacy rights

The abuse of Deepfake technology, such as using machine learning methods to create pornographic content, replacing facial features in pornographic videos without authorization, and spreading these tampered images to the internet, constitutes a new type of digital infringement that seriously damages the sexual privacy rights of victims.

2.3.2 Deepfakes: the proliferation of fakes

With the decreasing difficulty of obtaining Deepfake technology, its commercial application has become unstoppable. Some companies are beginning to use Deepfake methods to "splice" product advertisements, which is gradually evolving into a negative business competition situation.

2.3.3 Disruption of market order

Whether it is new opportunities brought by the popularity of technology or new frauds brought by synthetic audio, the mismatch between generation technology and detection technology will only lead

to the abuse of Deepfakes and ultimately cause disorder in market order. Because visual fake data is easier to be believed and remembered by the audience than any other modality of information, and can be used to fabricate future bank interest rate changes, liquidity crises or legal sanctions, traditional financial supervision mechanisms are unable to detect the involvement of Deepfakes.

2.3.4 The impact of Deepfake technology on social stability and democratic systems

(1) The authenticity of news is reduced. Deep forgery challenges visual authenticity, threatens news authenticity, and makes it difficult for videos to serve as a factual basis. The impact of Deepfake technology on news authenticity: imaginary; anyone can make news; profit-seeking behavior.

(2) Manipulation of public opinion and the chaos of information order. On social media, false information can easily manipulate public opinion, exacerbate conflicts, and trigger political information chaos and social unrest[1].

(3) Social trust faces a "deficit" crisis. Deepfake is easy to generate, AI information has strong appeal, and is easily favored by the public. When the public is immersed in various short videos that are precisely pushed according to their preferences, they will lose their objective understanding of the facts[9].

In other words, it will amplify or weaken the public's perception of the risks. Various media have gradually become "loudspeakers" for "risks". Once the public discovers this false information, they will no longer trust the media.

3. Deepfakes Policy in the United States

3.1 Policy background and legislative basis

The legislative foundation and background of Deepfake technology in the United States stem from deep concerns about privacy infringement, security threats, and potential abuse caused by artificial intelligence manipulation of content. To address these challenges, diverse legislative measures have been taken, with states such as California and Texas taking the lead by specifically enacting laws related to Deepfake content aimed at combating the spread of involuntary pornography and malicious behavior such as election interference.

3.1.1 The rise and application of Deepfake technology in the United States

The United States is at the forefront of Deepfake technology research and application.

In 2014, American AI expert Ian Goodfellow pioneered the GAN technology, which greatly enhanced the efficiency of Deepfakes and is of great milestone value.

The entertainment industry takes the lead in exploring the potential of Deepfake technology and leading the industry's development.

Popular apps such as Snapchat and TikTok have integrated Deepfake functionality to help users easily create and share fun videos.

Due to the risk of malicious misuse of this technology, the US Congress enacted the Deepfake Accountability Act in 2019.

3.1.2 Formulation of relevant policies

In December 2018, the US Senate introduced the Malicious Deepfakes Prohibition Act to crack down on malicious Deepfakes that mislead the public, with fines up to two years in prison. In 2019, the "Deep Counterfeiting Responsibility Act" was reviewed and proposed to mandate the addition of watermarks and descriptions to Deepfake content, but the legislation was not completed. In the same year, the Deepfake Reports Act was passed, requiring the Department of Homeland Security to report regularly. The United States has also introduced a series of regulations to clarify user responsibilities and severely punish abusive behavior.

At the state level, California was the first to ban the use of Deepfakes in election and pornography scenes; Virginia punishes unauthorized dissemination of Deepfakes. Texas legislates to restrict its application in the political field, while New York focuses on cracking down on its abuse in pornography. Maryland updates its child pornography laws to include crimes related to Deepfakes. In 2020, the GAN Output Identification Act required organizations such as NSF and NIST to strengthen

research on Deepfake identification technology and collaborate with the private sector to develop standards.

3.2 Supervision and Management Organization of Deepfake Technology

The United States has given technology giants such as Google and Microsoft, as well as local governments, greater power to control AI risks, and the federal government only intervenes when it is of significant interest. Before 2019, the United States mainly relied on local and industry self-regulation for Deepfakes, with relatively few federal regulations. Since 2019, the regulatory model has shifted from spontaneous indirect regulation to federal led direct regulation.

3.3 Supervisory measures and implementation status

Currently, the regulation of Deepfake technology in the United States mainly focuses on election fairness and personal privacy protection, while neglecting its widespread impact in daily life. Despite the public's awareness of its technology, the regulatory focus has led to a lack of understanding among the public. This imbalance may affect public perception, distort people's understanding of the hazards associated with Deepfake technology, and thus have a negative impact on social order[2].

4. Deepfakes Policy in the China

4.1 Policy background and legislative basis

Deepfake technology promotes the spread of false information and damages public opinion and trust. At the regulatory level, the 2017 Cybersecurity Law established the legal foundation for cyberspace governance, clarifying the importance of information authenticity and privacy protection. The Personal Information Protection Law and the 2021 Data Security Law strengthen data security and flow controllability. The Administrative Regulations on Internet Deep Forgery aims to curb technology abuse and reduce public interest damage.

4.1.1 The rise and application of Deepfake technology in China

Since 2017, Chinese tech companies and research institutions have actively invested in the development of Deepfake technology, applying it in fields such as film production, advertising, and virtual broadcasting. In 2021, China's Cyberspace Administration took regulatory measures on social networking software to address emerging risks associated with this technology. However, by 2023, online fraud rates remained high, with some perpetrators using Deepfake technology to conduct online transactions, successfully defrauding victims of over 2 million RMB.

4.1.2 Formulation of relevant policies

The Internet Audio and Video Regulations and other regulations require labeling of AI content and prohibit the misuse of deep learning technology. Multiple institutions have issued governance notices to standardize data collection, and the Civil Code protects portrait rights from forgery.

The draft and final regulations of the Integrated Management Regulations on Internet Information Services in 2022 strengthen the control of AI system. Additionally, the "Implementation Outline for a Rule of Law Society (2020-2025)" emphasized improving laws for AI and new media. Draft "Data Security Management Measures" required labeling synthesized content to prevent misuse, and a "Notice on Further Standardizing Online Audiovisual Programs" prohibited illegal content editing.

4.2 Supervision and Management Organization of Deepfake Technology

The Cyberspace Administration of China takes the lead in policy formulation, the Ministry of Industry and Information Technology is responsible for technical supervision, the public security department is in charge of criminal law enforcement, and the market supervision department is responsible for supervising application areas.

4.3 Supervisory measures and implementation status

In 2019, the government stipulated that when Tiktok, Kwai and other social platforms release Deepfake videos, they need to add eye-catching signs to indicate that the content is composite, and

require their users to bind their accounts with real name authentication.

In 2023, the government discovered a large number of fake advertisements created using Deepfake technology on the Douyin platform. The Cyberspace Administration of China has deleted Deepfake content and punished responsible parties. The police have uncovered a Deepfake telecommunications fraud case involving a total amount of 2 million yuan.

On February 29, 2024, the third-party agency Qi'anxin Group released "China's First Artificial Intelligence Security Report", which mentioned that in 2023, Deepfake fraud cases based on artificial intelligence surged by 3,000%.

5. Comparative analysis of Deepfake policies in the United States and China

5.1 Comparison of key issues in the formulation of laws and regulations on Deepfake technology between China and the United States

On Chinese side (see Figure 2 and Figure 3):

(1) National security and content recognition are the primary concerns, and technology control and content labeling systems are highly valued. (2) Privacy protection, platform responsibility, and prevention of AI abuse are also highly valued, while election integrity issues are relatively secondary. (3) The relevant regulations focus on maintaining national stability and technological security, and tend to adopt mandatory measures. (4) The Civil Code clearly protects the right to portrait, reflecting the importance of privacy protection.

On American side:

(1) Election integrity is regarded as a top priority, highlighting the maintenance of democratic system integrity. (2) The emphasis on privacy protection and content labeling is relatively balanced, while AI abuse and national security are relatively secondary. (3) The United States places greater emphasis on elections and individual rights, adopting a decentralized regulatory model that combines federal and state governments. (4) Although privacy protection is important, it relies more on individual case handling, and the content labeling system is relatively flexible, emphasizing industry self-discipline.

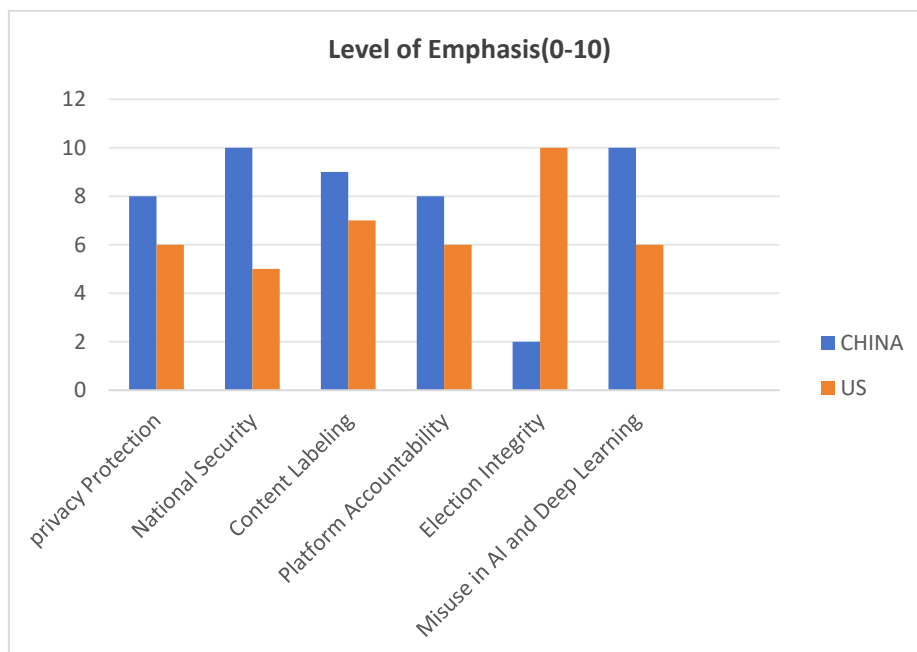


Figure 2 Level of Emphasis

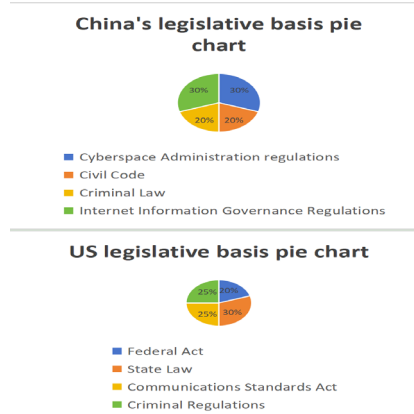


Figure 3 China's & US legislative basis pie chart

The regulatory framework for Deepfakes in China is constructed by the Cyberspace Administration of China, the Civil Code, the Criminal Law, and the Information Governance Regulations.

In the United States, it adopts a parallel approach of federal and state laws, with experimental bills at the federal level and state laws playing a key role in specific areas. At the same time, the Communication Standards Act and criminal law are also involved.

5.1.1 Regulatory measures

China attaches great importance to the regulation of Deepfake technology, and has established a regulatory system through measures such as mandatory labeling, protection of privacy portraits, development of technical standards, and strengthening platform responsibilities.

Some states in the United States restrict its application in specific scenarios, industries have self-discipline, and some platforms enjoy conditional exemptions. Although the federal government has paid attention to and started to develop regulatory standards, they have not yet been implemented (see Figure 4 and Figure 5).

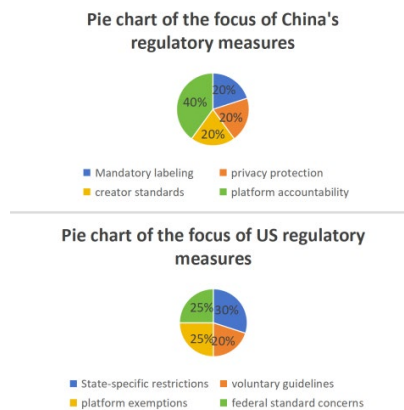


Figure 4 Pie chart of the focus of China's & US regulatory measures

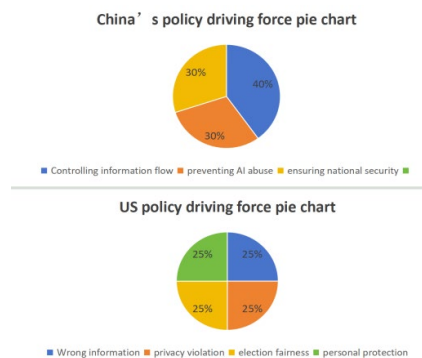


Figure 5 China's & US policy driving force pie chart

5.1.2 Policy Purpose

China focuses on information control, aiming to prevent the abuse of AI, ensure national security, and maintain network and public trust.

In the United States, due to issues such as misinformation, privacy, elections, and personal protection, regulation is relatively scattered, and each state has a certain degree of regulatory autonomy (see Figure 6).

	China	United States
Policy Background	The Chinese government prioritizes controlling information flow, preventing misuse of AI technologies, and protecting national security. The policies are shaped by the government's focus on cybersecurity and maintaining public trust.	The U.S. policy on Deepfakes is mainly driven by concerns over misinformation, privacy breaches, election integrity, and individual protection. U.S. regulation has been more fragmented with individual states (e.g., California, Texas) implementing their own Deepfake laws.
Legislative Basis	<ol style="list-style-type: none"> Cybersecurity Administration of China (CAC) regulations on AI and deep synthesis content. Civil Code of China: Covers privacy and reputation protections, relevant to Deepfake misuse. Criminal Law: include provisions against illegal digital content, potentially applying to harmful Deepfake content. Provisions on the Governance of Online Information Content (2020): Addresses AI-generated content as part of online information governance. 	<ol style="list-style-type: none"> Federal Initiatives: No comprehensive federal law yet, but attempts have been made (e.g., Deepfakes Accountability Act). State Laws: California's AB 730 and AB 602 prohibit the use of Deepfakes in political and pornographic contexts. Communications Decency Act (Section 230): Grants platforms immunity from third-party content but may see amendments to address Deepfake harms. Criminal statutes: Applied in cases involving fraud or harm.
Policy Content	<ol style="list-style-type: none"> Mandatory labeling of AI-generated content. Chinese regulations require labeling to differentiate AI-generated content. Privacy and image rights: Regulations prioritize individual consent, particularly in cases of altered video or image content. Technical standards for content creators: Deepfake creators must follow specific technical standards, including safeguards for responsible AI use. Platform accountability: Chinese platforms are liable for monitoring Deepfake content, implementing safety protocols, and removing harmful content. 	<ol style="list-style-type: none"> Restricted use in specific contexts: California and Texas laws focus on Deepfake restrictions in elections and explicit content without consent. Voluntary industry guidelines: Some U.S. tech companies adopt guidelines for AI content, including labeling and user consent. Platform immunity with exceptions Emerging federal guidance: Initial federal interest in setting standards for Deepfake technology use, especially in national security contexts, but no mandate yet on labeling or content removal.

Figure 6 Comparison of policy background and legislative basis

5.2 Policy implementation and effect comparison

To gain insights into the public's understanding of and attitudes toward Deepfake technology and its regulation, we conducted a survey that gathered responses from two groups of participants based on their country of residence. In total, we collected 67 completed questionnaires: 37 from respondents born and residing in China and 30 from respondents residing in the United States. This data will enable us to compare perceptions and awareness levels of Deepfake technology across these two distinct national contexts, as well as evaluate their views on regulatory measures and the effectiveness of current policies in managing Deepfake risks.

5.2.1 Comparison of understanding of Deepfake technology

Chinese respondents generally have a higher level of understanding of Deepfake technology, while American respondents have a lower level of knowledge.

In China, the majority of respondents have a high level of self-evaluation awareness, while a few consider it low; There are significant differences in opinions regarding regulation, but the majority support regulators.

In the United States, respondents have a relatively balanced rating of Deepfake technology and hold a stronger supportive attitude towards the necessity of regulation.

5.2.2 Comparison of Views of the two countries on policy effectiveness

The average rating of Chinese respondents on the effectiveness of Deepfake regulatory policies is 2.89, close to the mean, indicating doubts about the policy's effectiveness; However, American respondents scored slightly higher at 3.48, indicating greater confidence in government regulation.

Both Chinese and American respondents share the same view on the necessity of regulating online shopping. But when faced with Deepfake issues, American respondents have more confidence in the government's response measures.

Both countries' respondents expressed support for the proposal to establish policies to improve regulatory efficiency, with Chinese respondents scoring higher, reflecting a stronger demand for relevant policies.

6. Lessons learned from the experiences of two countries

6.1 Quantitative evaluation of policy implementation effectiveness

To quantitatively evaluate the effectiveness of policies, the plan is to first calculate the scores of

each sub item in the questionnaire, and based on this, design a quantitative evaluation index ranging from 1 to 5 points as a benchmark for measuring the effectiveness of policies.

Next, the average score of all issues for each country will be calculated to obtain a "Deepfake Policy Effectiveness Comprehensive Score", which is presented as a single value ranging from 1 to 5, comprehensively reflecting the overall effectiveness of the policy.

For the policy effectiveness questions, the scores were calculated by combining Likert ratings (A 5-point Likert scale is used here: 1 indicates very low effectiveness, 5 indicates very high effectiveness)

China and the U.S. indicate moderate effectiveness in each country's Deepfake policy, with scores around 2.6 on a scale from 1 to 5. (2.6 suggests a level of effectiveness slightly above minimal but far from fully effective, indicating that respondents perceive room for significant improvement in policy measures.)

6.2 Public Awareness and Education

6.2.1 US cases and reference significance

In the United States, improving the public's awareness and ability to identify Deepfake technology is an important part of dealing with the risk of Deepfakes. For example, California legislators have approved a number of bills aimed at improving AI literacy, including a call for the establishment of a state working group to explore the possibility of incorporating AI skills into various educational courses such as mathematics, science, history and social sciences, so as to enhance the public's, especially students', understanding of Deepfake technology and help them learn to identify false information.

In addition, some American technology companies and social organizations will jointly carry out publicity activities to popularize the principles, common application scenarios and possible risks of Deepfake technology to the public through online and offline lectures, popular science videos, etc.

6.2.2 Chinese cases and reference significance

In China, the cyber security department and educational institutions jointly launched the Cyber security Campus Campaign, which popularized cyber security knowledge to students through knowledge competitions, including the possible harm caused by Deepfake technology and how to identify it.

6.3 Regulatory model

6.3.1 US cases and reference significance

The United States has given technology companies and local governments greater power in regulating Deepfake technology. With their strong technical strength and resources, these companies can quickly use their own algorithms and other technical means to monitor and identify relevant content on their platforms when dealing with Deepfake technology, and can promptly discover and deal with some Deepfake information.

Regarding local governments, each state in the United States can formulate corresponding policies based on its own local conditions and public needs.

6.3.2 Chinese cases and reference significance

For China, this regulatory model is worth learning from. China can further refine the rules and mechanisms for industry self-regulation on the basis of ensuring the unity of the country's overall regulatory framework. Internet technology companies can also be encouraged to actively participate in Deepfake technology supervision, so as to give full play to their advantages in technology research and development, data processing and so on. It is necessary to develop more efficient and accurate Deepfake content Detection Tools, and formulate industry-specific Deepfake content processing standards and self-discipline codes through industry associations and other organizations to guide enterprises to consciously fulfill their social responsibilities and strengthen the management of their own platform content.

6.4 Challenges

6.4.1 Legal differences

The significant legal differences between China and the United States hinder the mutual learning and implementation of deeply false policies. For example, the "sentencing standards" of different states in the United States vary in the severity of sentencing for Deepfake-related crimes, which is influenced by many factors such as the state's legal traditions and social concepts. China, on the other hand, has a unified criminal law framework that imposes penalties in accordance with established sentencing standards based on the nature of the criminal behavior and the severity of the circumstances.

6.4.2 Differences in technological development

The United States has always been at the forefront of artificial intelligence technology, and started research and development of Deepfake technology earlier, and has advantages in some advanced algorithm research, software tool development, etc. China has developed relatively slowly in technology.

6.4.3 Sociocultural differences

American culture advocates individualism and freedom, and privacy protection is often approached from an individual perspective. The public highly expects freedom of speech and creation in cyberspace.

In contrast, Chinese culture emphasizes collectivism, focuses on collective interests and social harmony, and is more alert to the potential social order chaos and public opinion misguidance caused by Deepfake technology. Therefore, in policy-making, it tends to strictly limit its scope of use.

7. Conclusion

The two countries should continue to improve their respective Deepfake policies. The United States can further integrate the scattered laws and regulations of each state to build a more unified and comprehensive federal-level Deepfake technology supervision system. On the basis of maintaining the existing advantages of multi-departmental collaborative supervision, China continues to optimize the supervision process and improve supervision efficiency. At the same time, according to the development of technology, it timely updates and refines relevant application specifications to strengthen the precise control of the application of Deepfake technology in different industries.

References

- [1] Zelenkauskaitė, A. (2022). *Creating chaos online: Disinformation and subverted post-publics*. Ann Arbor: University of Michigan Press.
- [2] Rød B, Pursiainen C, Eklund N. (2025). *Combatting Disinformation — How Do We Create Resilient Societies? Literature Review and Analytical Framework*. *European Journal for Security Research*, (1), 1-43.
- [3] Clive Thompson. *What the History of Spirit Photography' Portends for the Future of Deepfake Videos*. Available from: <https://www.smithsonianmag.com/innovation/history-spirit-photography-future-Deepfake-videos-180979010/>.
- [4] Arnold. *The History of Deepfake Technology: How Did Deepfakes Start?* Available from: <https://Deepfakenow.com/history-Deepfake-technology-how-Deepfakes-started/>.
- [5] Rossler A, Cozzolino D, Verdoliva L, et al. *Faceforensics: A large-scale video dataset for forgery detection in human faces*. Available from: <http://arxiv.org/pdf/1803.09179>.
- [6] Chesney, R., & Citron, D. K. (2019). *Deep fakes: A looming challenge for privacy, democracy, and national security*. *California Law Review*, 107, 1753-1819.
- [7] Nyilasy, G. (2019). *Advertising and the post-truth world: A reflection on misinformation, disinformation, and fake news*. In B. Dahlen & M. Rosengren (Eds.), *Marketing and the common good: Essays from the 3rd Marconi Conference*. Stockholm: Stockholm School of Economics Institute for Research.
- [8] Nyilasy, G. (2019). *Epistemic defense of advertising: Inoculation theory, fake news, and public policy*. *Journal of Advertising*, 48(2), 176-186.
- [9] Liu, M. (2023). *The "intelligent deception" of deepfakes and digital governance*. Master's thesis. Guangzhou: Guangzhou University.