January 2026

CCIA Comments on Japan's Draft Principle-Code on Generative AI Transparency and Intellectual Property

Introduction

The Computer & Communications Industry Association (CCIA)[1] welcomes the opportunity to comment on the draft "Principle-Code for Protection of Intellectual Property and Transparency for the Appropriate Use of Generative AI,"[2] issued by Japan's Intellectual Property Strategy Headquarters in December 2025.[3]

The Principle-Code is presented as a soft-law implementation measure under the Act on Promotion of Research, Development and Utilization of Artificial Intelligence-Related Technologies (Act No. 53 of 2025),[4][5] which entered into effect in November 2025.[6] Rather than creating new statutory obligations, it seeks to advance the Act's objectives on transparency and intellectual property (IP) protection through voluntary compliance reinforced by reputational and market-based incentives.

CCIA supports transparency regarding AI data inputs and has contributed[7] to consensus-based international efforts, including standards promoted through the Hiroshima AI Process (HAIP). However, transparency measures must be technically feasible and proportionate. Against the backdrop of the development of voluntary international standards (*e.g.*, ISO/IEC 12792:2025), Japan's shift toward more prescriptive EU-style disclosure requirements risks undermining its commitment to an innovation-friendly AI policy environment.

As the government finalizes the Principle-Code, the framework must support Japan's broader AI policy objectives. The scope and prescriptiveness of certain disclosure obligations—particularly dispute-triggered information requests—could create uncertainty for globally operating developers and providers. If misaligned, these requirements risk slowing AI deployment in Japan, contrary to the government's stated goal of lowering barriers to AI adoption and strengthening Japan's position as a leading environment for AI development.

---

[1] For more than 50 years, CCIA has promoted open markets, open systems, and open networks. CCIA members employ more than 1.6 million workers, invest more than $100 billion in research and development, and contribute trillions of dollars in productivity to the global economy. A list of CCIA members is available at https://www.ccianet.org/members.

[2] https://public-comment.e-gov.go.jp/pcm/download?seqNo=0000305363

[3] https://public-comment.e-gov.go.jp/pcm/detail?CLASSNAME=PCMMSTDETAIL&id=095251270&Mode=0

[4] https://laws.e-gov.go.jp/law/507AC0000000053

[5] https://www.kojimalaw.jp/wp/wp-content/uploads/2025/09/Japan-AI-Promotion-Act-KOJIMA-LAW-OFFICES-jp-en-reference-translation.pdf

[6] https://www.gov-online.go.jp/hlj/en/november_2025/november_2025-08.html

[7] See https://ccianet.org/wp-content/uploads/2025/01/Principles-and-Template-Transparency-in-AI-Model-Training-Data.pdf

Key Industry Concerns

Risk of *De facto* Mandatory Effects Despite Voluntary Framing

Although technically voluntary, the comply-or-explain model—when combined with informal pressure to adopt the code and public listing of participating companies and their disclosures—risks creating *de facto* mandatory standards. Numerous elements of the proposed code are framed as "requirements," and within the framework are treated as both mandatory and highly prescriptive.[8] Market expectations, litigation exposure, and pressure from regulators and business partners may make it difficult for U.S. companies to meaningfully deviate from the principles without reputational or commercial consequences.

Protection of Trade Secrets and Sensitive Technical Information

The scope and granularity of Principle 1 disclosures exceed existing transparency norms and risk conflicting with established protections for trade secrets under Japanese law, including the Unfair Competition Prevention Act.[9] Even high-level descriptions of model architecture, training methods, data sourcing practices, and crawler operations may expose sensitive information about proprietary systems, security safeguards, or business strategy. The repeated emphasis that trade secret concerns should not automatically justify non-disclosure, coupled with expectations for detailed explanations when companies decline to comply, heightens the risk of compelled disclosure of competitively sensitive information. In many cases, mandatory disclosure of technical details (including model architecture and computing hardware) bears little relevance to the stated objective of copyright protection.

Operational and Legal Burdens of Dispute-Triggered Disclosures

Principles 2 and 3 introduce disclosure pathways alongside existing civil procedure tools, raising technical, operational, and due process concerns. Although framed as limited to easily confirmable information (e.g. specific URLs), responding to individualized requests at scale would impose substantial burdens on developers and does not reflect the technical realities of large-scale model training.

Additionally, generative AI models do not store or retrieve source materials as discrete records; they learn statistical relationships from vast datasets, with individual data points making minimal and non-traceable contributions, rendering source-level attribution infeasible. Moreover, these requirements may conflict with privacy protective policies implemented by some model providers that limit logging or retention of user prompts and outputs.

Moreover, requiring disclosures in response to parties merely contemplating legal action shifts preliminary assessments of claim legitimacy from courts to AI providers, creating opportunities for strategic requests, evidence gathering outside formal discovery, and inconsistent or duplicative demands despite nominal safeguards. Although the principles recognize risks of abusive requests and the need for reasonableness, their net effect is

[8] *E.g.,* Principles 1 and 2 both contain extensive lists of items that "shall be disclosed."
[9] https://www.japaneselawtranslation.go.jp/en/laws/view/2803/en

likely a massive increase in compliance burdens with no obvious benefits beyond facilitating litigation.

Chilling Effects on Lawful Data Use and Innovation

By linking transparency obligations with requirements for how companies prevent, monitor, and respond to potential IP issues during training and output generation, the framework risks reopening substantive copyright questions that Japan has historically addressed in a relatively innovation-friendly manner.[10] Emphasis on commitments to avoid IP infringement during training, combined with similarity-based disclosure triggers, may create uncertainty around lawful data use and discourage beneficial model development, as Japan seeks to accelerate AI adoption and close the gap with leading AI economies.[11]

These concerns are amplified by the interaction between the draft Principle-Code and Japan's existing copyright framework. Japan has long provided legal certainty for machine learning through its Copyright Act, including provisions permitting the use of copyrighted works for data analysis. By reintroducing questions about training legality through disclosure and transparency mechanisms—rather than legislative reform—the draft risks undermining this certainty and re-litigating settled policy choices through soft-law expectations rather than statutory process.

Fragmentation

The draft applies to generative AI systems and services provided in Japan, regardless of where the developer or provider is located. This approach is inconsistent with Japan's copyright framework and international laws, including the Berne Convention and TRIPS,[12] which are built on the principle that copyright is territorial in nature. For multinational companies, extraterritorial application of the Principle-Code raises the risk of fragmented compliance obligations and Japan-specific disclosure practices that may not align cleanly with other jurisdictions' more flexible, risk-based frameworks. In contrast, internationally recognized models like the OECD principles[13] prioritize interoperability, outcome-based governance, and adaptability over prescriptive disclosure mandates. Absent clearer alignment with such models, ongoing uncertainty about future revisions tied to evolving international trends further complicates long-term compliance planning.

Extraterritoriality

The potential extraterritorial application of the draft Principle-Code raises significant concerns regarding its impact on the AI ecosystem. By extending its obligations to generative AI systems and services provided in Japan—regardless of the developer's or provider's location—the framework introduces significant compliance complexity and operational burdens for multinational companies. Such broad scope, without clear mechanisms for recognizing equivalent compliance efforts in other major jurisdictions, risks forcing global providers to

[10] https://www.nishimura.com/sites/default/files/newsletters/file/robotics_ai_230711_en.pdf
[11] https://project-disco.org/innovation/balancing-risk-and-innovation-ai-governance-strategies/
[12] https://www.wto.org/english/tratop_e/trips_e/intel2_e.htm
[13] https://www.oecd.org/en/topics/sub-issues/ai-principles.html

create Japan-specific versions or compliance protocols for their general-purpose AI models. This approach not only increases the cost and time of deployment in Japan but also sets a precedent for divergent national rules, ultimately undermining the goal of global interoperability and standard-setting that Japan has supported through forums like the Hiroshima AI Process. The effect is a disproportionate regulatory reach that would compel non-Japanese entities to adhere to prescriptive requirements that conflict with or duplicate obligations in their home countries, creating a chilling effect on the deployment of state-of-the-art AI systems within Japan's market.

Recommendations

The draft Principle-Code is central to Japan's effort to promote trustworthy AI and position itself as a global leader in AI development and governance. However, its current scope and prescriptiveness risk increasing uncertainty and operational burdens, diverging from internationally aligned approaches and potentially undermining AI innovation and adoption.

1. Clarifying Disclosure Scope Under Principle 1

First, the scope and granularity of disclosures under Principle 1 should be narrowed and clarified to focus on information directly relevant to transparency and trust, while explicitly excluding details that could compromise trade secrets or cybersecurity. Guidance should confirm that high-level, qualitative disclosures are sufficient, and that companies may rely on existing public materials or internationally recognized transparency reporting where appropriate.

2. Aligning Principles 2 & 3 with Due Process and Technical Feasibility

Disclosure mechanisms under Principles 2 and 3 should be revised to better respect due process and technical feasibility. The Principle-Code should clarify that AI providers are not expected to assess the legal merit of potential claims or to provide source-level attribution that is infeasible in large-scale models. Disclosure obligations should be limited to information that is reasonably accessible, verifiable, and relevant, and must not substitute judicial discovery or established civil procedure. Additional safeguards are needed to prevent strategic or abusive requests, including clearer eligibility thresholds and greater deference to existing legal processes.

3. Preserving Legal Certainty Under Copyright Law

The Principle-Code should recognize Japan's existing copyright framework, including provisions that permit lawful data analysis for machine learning. Transparency and disclosure expectations should not reopen settled questions about the legality of training practices through soft-law mechanisms. Maintaining legal certainty is critical to sustaining investment, innovation, and adoption, particularly in content-rich sectors where Japan leads globally.

4. Ensuring International Alignment

Finally, to avoid fragmentation and duplicative compliance burdens, the government should align with international law and respect the principle of state sovereignty by avoiding extraterritorial obligations and establishing a clear mechanism recognizing disclosures made under internationally aligned frameworks. Transparency measures consistent with global processes—particularly those Japan has helped promote through international initiatives—should be sufficient to satisfy the Principle-Code. This would reinforce Japan's leadership in global AI governance, promote cross-jurisdictional interoperability, and preserve flexibility for diverse technologies and business models, while continuing to advance trust and accountability.

Conclusion

CCIA supports Japan's objective of promoting trustworthy generative AI while reinforcing its position as a global leader in AI development and governance. To achieve these goals while supporting innovation, adoption, and global competitiveness, the framework should be carefully calibrated to avoid unintended legal, technical, and operational consequences. Refining disclosure expectations, anchoring dispute-related mechanisms in established legal processes, maintaining legal certainty, and aligning with international frameworks would strengthen the Principle-Code and reinforce Japan's leadership in the global AI ecosystem. CCIA appreciates the opportunity to submit these comments and remains available for further dialogue as the Japanese government considers next steps.