Asia Pacific Perspectives

Published in June 2026

Table of Contents

Chief Editor
Dr. Alex Hsu
(Director General, CTPECC)

Editorial Committee
Dr. Shunyo Liao
(Professor, National Chung Hsing University)
Dr. Chen-Sheng Ho
(Research Fellow, Department of International Affairs, TIER)

Editor
Austin Chou
(Assistance Research Fellow, CTPECC)
Louisa Wu
(Assistant Research Fellow, CTPECC)

About the CTPECC

CTPECC is a full member of Pacific Economic Cooperation Committee (PECC), which is an international organization for economic cooperation in the Asia-Pacific region and plays a key role in consultation and advice on APEC's major initiatives and plans. The participation of CTPECC is to assist the government in researching and analyzing economic cooperation plans, and to strive for greater opportunities to participate in cooperation mechanisms and dialogues.

Digital Governance for Inclusive AI Communities: APEC's Pathway to Shared Prosperity in the Asia-Pacific

Kai-Hsin Chang
Assistant Professor /
Director of Research Center for the Legal Regime of Artificial Intelligence at the College of Law, Tunghai University

Introduction: From Digital Transformation to Inclusive Governance

The Asia-Pacific is entering a new phase of digital transformation. Artificial intelligence, data-driven services, digital payments, cloud infrastructure, and platform-based markets are reshaping how people work, trade, learn, receive public services, and participate in society. Yet the central policy question is no longer whether economies should adopt digital technologies. It is how digital transformation can be governed so that its benefits are broadly shared across communities, enterprises, regions, and generations.

This question fits squarely within APEC 2026's theme, "Building an Asia-Pacific Community to Prosper Together," and its priorities of openness, innovation, and cooperation.[1] This framing also reflects APEC's longer-term agenda under the Putrajaya Vision 2040 and the Aotearoa Plan of Action, which link innovation and digitalization with strong, balanced, secure, sustainable, and inclusive growth.[2] In the AI era, prosperity together cannot be achieved by technological diffusion alone. It requires governance together: shared principles, interoperable standards, trusted data flows, digital public infrastructure, inclusive skills policies, and mechanisms for accountability. Digital governance should therefore be understood not merely as regulation of technology, but as the institutional design that determines who can access digital

1. Asia-Pacific Economic Cooperation, "China Unveils APEC 2026 Theme and Priorities in Shenzhen," December 12, 2025, accessed May 27, 2026, https://www.apec.org/press/news-releases/2025/china-unveils-apec-2026-theme-and-priorities-in-shenzhen.
2. Asia-Pacific Economic Cooperation, "APEC Putrajaya Vision 2040," 2020 APEC Economic Leaders' Declaration, November 20, 2020, accessed May 27, 2026, https://www.apec.org/Meeting-Papers/Leaders-Declarations/2020/2020_aelm/Annex-A; Asia-Pacific Economic Cooperation, "Annex: Aotearoa Plan of Action," 2021 APEC Economic Leaders' Declaration, November 12, 2021, accessed May 27, 2026, https://www.apec.org/meeting-papers/leaders-declarations/2021/2021-leaders-declaration/annex-aotearoa-plan-of-action

opportunities, who is protected from digital harms, and who has a voice in shaping digital futures.

For APEC and PECC communities, the challenge is especially complex. The region includes advanced digital economies, emerging markets, large platform ecosystems, small and medium-sized enterprises, remote communities, aging societies, and diverse legal traditions. A common digital governance agenda must therefore avoid a one-size-fits-all model. Instead, it should create practical pathways for interoperability, trust, and capacity building while respecting different domestic contexts.

Why Inclusion Matters in the AI Economy

AI can accelerate productivity, improve public services, enhance disaster response, support healthcare, strengthen supply-chain resilience, and help small businesses reach new markets. However, AI can also widen existing inequalities. Communities with limited broadband access, weak digital literacy, fewer data resources, or lower institutional capacity may be excluded from AI-enabled growth. Small firms may lack the capital or technical expertise to adopt AI responsibly. Workers may face displacement without sufficient reskilling pathways. Public agencies may deploy automated systems without adequate transparency, contestability, or human oversight.

Inclusion must therefore be treated as a core design requirement, not a secondary social objective. The Asian Development Bank has cautioned that digital transformation may exacerbate inequality if it is not carefully managed, and that public policies are needed to address market and equity failures while embedding inclusion and sustainability goals.[3] This insight is particularly important for AI governance. AI systems are shaped by data, models, infrastructure, and deployment contexts. If data are incomplete, communities are underrepresented, or administrative processes lack remedies, AI can reproduce or amplify social exclusion.

An inclusive AI community is not simply a population of users connected to digital services. It is a governance ecosystem in which people, firms, governments, and civil society can participate safely and meaningfully. Inclusion requires affordable access, usable services, multilingual and accessible interfaces, trusted identity and payment systems, cybersecurity protections, data rights, and institutional channels for feedback and redress.

APEC's Digital Governance Foundation

APEC already has a useful foundation for this agenda. The APEC Internet and Digital Economy Roadmap describes itself as a living document to guide cooperation on the internet and digital economy, while recognizing the diversity of economic and social circumstances across APEC economies.[4] The 2025 APEC Digital and AI Ministerial Statement further encouraged members to use applicable digital governance mechanisms to promote dialogue and to explore collaborative approaches so that ICT and digital innovation benefit people and the region.[5]

3. Asian Development Bank, Harnessing Digital Transformation for Good: Asian Development Policy Report (Manila: Asian Development Bank, 2025), 9–10, 24–25, accessed May 27, 2026, https://www.adb.org/publications/asian-development-policy-report-2025.
4. Asia-Pacific Economic Cooperation, APEC Internet and Digital Economy Roadmap, finalized version, October 24, 2017, 1, accessed May 27, 2026, https://www.apec.org/docs/default-source/Groups/ECSG/17_csom_006.pdf.
5. Asia-Pacific Economic Cooperation, "2025 APEC Digital and AI Ministerial Statement," August 4, 2025, para. 13, accessed May 27, 2026, https://www.apec.org/meeting-papers/sectoral-ministerial-meetings/telecommunicationsandinformation/2025-apec-digital-and-ai-ministerial-statement.

These documents point toward a practical regional approach: APEC should not seek to impose a single AI law or centralized digital model. Rather, it can help economies align around functional principles: trust, openness, interoperability, accountability, resilience, and capacity building. Such principles are consistent with international developments. The OECD Recommendation of the Council on Artificial Intelligence, which established the OECD AI Principles as the first intergovernmental standard on AI, promotes the responsible stewardship of trustworthy AI in a manner that supports innovation while respecting human rights and democratic values; it was revised in 2024 to reflect technological and policy developments, including those related to generative AI.[6] NIST's AI Risk Management Framework provides a voluntary, rights-preserving, and use-case-agnostic framework for managing risks associated with AI systems,[7] while ISO/IEC 42001 specifies requirements and guidance for establishing, implementing, maintaining, and continually improving an AI management system within an organization.[8]

For APEC, the value of these frameworks is not that they should be copied mechanically. Their value is that they help translate high-level principles into governance practices: risk mapping, documentation, impact assessment, monitoring, accountability, incident management, and continuous improvement. These are exactly the tools needed to make AI governance inclusive and operational.

Three Pillars for Inclusive Digital Governance

A practical APEC agenda for inclusive digital governance can be built around three pillars.

Pillar One: Trustworthy AI and Data Governance

First, APEC economies should strengthen trustworthy AI and data governance. AI systems depend on data, and data governance determines whether digital innovation can be both dynamic and trusted. This includes privacy protection, cybersecurity, lawful data sharing, data quality, transparency, and mechanisms for individuals and communities to challenge harmful outcomes. For APEC, this data-governance agenda can build on existing regional instruments such as the APEC Privacy Framework and the APEC Cross-Border Privacy Rules system, which seek to protect personal information while maintaining cross-border information flows through accountability-based and interoperable privacy mechanisms.[9]

For businesses, especially SMEs, trustworthy AI governance should not be framed only as compliance cost. It can become a market enabler. Firms that can demonstrate responsible AI management, cybersecurity readiness, and reliable data practices

6.Organisation for Economic Co-operation and Development, Recommendation of the Council on Artificial Intelligence, OECD/LEGAL/0449, adopted May 22, 2019, amended May 3, 2024, 3–4, accessed May 27, 2026, https://legalinstruments.oecd.org/api/print?ids=648&lang=en.

7.National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (Gaithersburg, MD: National Institute of Standards and Technology, January 2023), 2, 4, 20–21, accessed May 27, 2026, https://doi.org/10.6028/NIST.AI.100-1.

8.International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 42001:2023, Information Technology—Artificial Intelligence—Management System (Geneva: ISO/IEC, 2023), vi, 1, accessed May 27, 2026, https://www.iso.org/standard/42001.

9.Asia-Pacific Economic Cooperation, APEC Privacy Framework (2015) (Singapore: APEC Secretariat, 2017), 2–4, 31, accessed May 27, 2026, https://www.apec.org/publications/2017/08/apec-privacy-framework-%282015%29; Asia-Pacific Economic Cooperation, APEC Cross-Border Privacy Rules System: Policies, Rules and Guidelines (2015), 2–6, 14, accessed May 27, 2026, https://www.apec.org/docs/default-source/Groups/ECSG/CBPR/CBPR-PoliciesRulesGuidelines.pdf.

will be better positioned to join cross-border digital supply chains. Standards such as ISO/IEC 42001 and risk-based tools such as the NIST AI RMF can help firms translate responsible-AI principles into documented, risk-based, and reviewable management practices, including audit-ready processes where appropriate.[10]

For governments, trustworthy AI governance should focus on public accountability. When AI is used in public services, citizens should know when automated tools are involved, what purposes they serve, what data are used, and how decisions can be reviewed. Human oversight, appeal mechanisms, procurement standards, and audit trails are essential. Without these safeguards, AI may improve administrative efficiency while weakening public trust.

Pillar Two: Inclusive Digital Public Infrastructure

Second, economies should invest in inclusive digital public infrastructure. Digital public infrastructure refers to foundational digital systems such as digital identity, payment systems, and secure data exchange layers. UNDP emphasizes that digital public infrastructure—such as digital identity, payments, and data-exchange systems—can make everyday services more connected and inclusive, and that safe, fair, and interoperable digital systems can accelerate progress toward the Sustainable Development Goals.[11]

For inclusive communities, DPI should be designed as public-interest infrastructure rather than merely technical architecture. It should enable access to healthcare, education, social protection, financial services, licensing, trade facilitation, and disaster relief. It should also be accessible to older adults, persons with disabilities, rural communities, micro-enterprises, and people with limited digital skills.

The governance of DPI is as important as its deployment. Poorly governed infrastructure can create surveillance risks, exclusion through authentication failures, vendor lock-in, cybersecurity vulnerabilities, or unequal access. The Universal DPI Safeguards Framework therefore emphasizes safeguards across the DPI life cycle to mitigate risks to safety and inclusion, including privacy vulnerability, digital insecurity, lack of recourse, discrimination, unequal access, exclusion, and disempowerment.[12] Inclusive DPI should accordingly be guided by proportional data use, privacy by design, cybersecurity by design, open standards where appropriate, independent oversight, effective redress, and user-centered service design.

Pillar Three: Regional Interoperability and Capacity Building

Third, APEC should advance regional interoperability and capacity building. The Asia-Pacific digital economy depends on cross-border trust: trusted data flows, interoperable identity credentials, compatible cybersecurity practices, reliable digital trade documentation, and mutual learning on AI governance. Fragmented rules can

10. International Organization for Standardization and International Electrotechnical Commission, ISO/IEC 42001:2023, Information Technology—Artificial Intelligence—Management System (Geneva: ISO/IEC, 2023), 6–16, 17–20; National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework (AI RMF 1.0), NIST AI 100-1 (Gaithersburg, MD: National Institute of Standards and Technology, January 2023), 20–32, accessed May 27, 2026, https://doi.org/10.6028/NIST.AI.100-1.
11. United Nations Development Programme, "Digital Public Infrastructure," UNDP Digital, accessed May 27, 2026, https://www.undp.org/digital/digital-public-infrastructure.
12. Office of the UN Secretary-General's Envoy on Technology and United Nations Development Programme, The Universal Digital Public Infrastructure Safeguards Framework: A Guide to Building Safe and Inclusive DPI for Societies (New York: UN OSET and UNDP, September 2024), 4–6, 12–15, 22–25, accessed May 27, 2026, https://framework-dpi-safeguards.org/frameworkpdf.

raise costs for SMEs and limit the diffusion of innovation.

Interoperability does not mean identical laws. It means that different systems can communicate, recognize comparable safeguards, and support cross-border cooperation. APEC is well suited to this task because it has a tradition of voluntary, non-binding, consensus-based cooperation. This allows economies to pilot practical tools, share policy lessons, and develop capacity without requiring immediate legal harmonization. This platform role is reflected in APEC's implementation of the Internet and Digital Economy Roadmap through the Digital Economy Steering Group: the 2025 DESG Chair's Report notes that AIDER supports the Putrajaya Vision 2040's innovation-and-digitalisation agenda and that, in 2025, more than 110 digital-economy initiatives were implemented across over 25 APEC fora and sub-fora.[13]

Capacity building should focus on three groups. The first is public officials who must procure, regulate, and oversee AI systems. The second is SMEs that need affordable tools for responsible AI adoption. The third is communities and workers who need AI literacy, digital skills, and social protection pathways. Without these investments, AI governance may become a conversation among experts while communities experience technology as something imposed upon them.

The Role of Chinese Taipei

Chinese Taipei can make meaningful contributions to this regional agenda. Its strengths in semiconductors, ICT supply chains, cybersecurity, digital government, healthcare technology, and SME innovation provide practical experience relevant to APEC's inclusive digital governance work. In APEC digital cooperation, Chinese Taipei can support capacity building in responsible AI adoption, digital resilience, data governance, and SME digital transformation, including through APEC project-based cooperation on SME digital innovation and green supply-chain competitiveness.[14]

The most valuable contribution may be a bridge-building role. Chinese Taipei's economy combines advanced technological capacity with deep SME networks. This allows it to demonstrate how AI governance can be translated into practical tools for enterprises that do not have large legal, technical, or compliance departments. APEC's inclusive growth agenda will not succeed if responsible AI remains feasible only for large corporations. Governance must be simplified, modular, and scalable for smaller firms.

Chinese Taipei can also contribute to trusted digital public services. Lessons from digital identity, health data governance, cybersecurity drills, and public-private technology partnerships can help shape APEC dialogues on inclusive DPI. These experiences are particularly useful when linked to regional capacity building rather than presented as a single model for others to adopt.

Policy Recommendations

To move from principle to implementation, APEC and PECC communities could consider five policy directions.

13. Asia-Pacific Economic Cooperation, Digital Economy Steering Group Chair's 2025 Report on the Implementation of the APEC Internet and Digital Economy Roadmap (AIDER), 2025/CSOM/003, October 2025, 1–4, accessed May 27, 2026, https://mddb.apec.org/Documents/2025/SOM/CSOM/25_csom_003.pdf.
14. Asia-Pacific Economic Cooperation, APEC Digital Innovation to Enhance SMEs Competitiveness in Green Supply Chains Initiative, SMEWG_104_2024A, APEC Project Proposal, 2024, 1–3, 6–7, accessed May 27, 2026, https://pdb.apec.org/Lists/Proposals/DispForm.aspx?ID=6634.

First, APEC could develop an Inclusive AI Governance Toolkit. This toolkit would not be a binding regulation. It could provide practical checklists for AI impact assessment, data quality, human oversight, procurement, transparency, accessibility, and grievance mechanisms. Separate modules could be designed for governments, SMEs, and civil society organizations.

Second, APEC could launch an SME Responsible AI Adoption Sandbox. Many SMEs want to use AI for translation, customer service, logistics, marketing, compliance, and productivity, but they lack risk-management resources. A sandbox could provide templates, mentoring, shared testing environments, and sector-specific examples.

Third, APEC could promote trusted data-sharing frameworks for public-interest use cases, such as disaster response, public health, climate adaptation, fraud prevention, and supply-chain resilience. These frameworks should include privacy safeguards, cybersecurity requirements, purpose limitation, and accountability mechanisms.

Fourth, APEC could support AI and digital literacy for inclusive communities. This should go beyond coding education. It should include understanding automated decisions, recognizing AI-generated misinformation and deepfakes, protecting personal data, using digital public services, and participating in policy consultations.[15]

Fifth, APEC could encourage interoperable standards and assurance mechanisms. International standards and risk frameworks can help economies and firms communicate trust across borders. However, assurance should remain proportionate. Overly burdensome certification may exclude SMEs, while weak assurance may undermine public confidence. The goal should be tiered governance: higher-risk systems require stronger controls, while lower-risk uses receive simpler guidance.

Conclusion: Prosperity Together Requires Governance Together

Digital transformation will not automatically create inclusive communities. AI can generate new prosperity, but it can also deepen divides if governance is weak, fragmented, or inaccessible. The Asia-Pacific therefore needs a digital governance agenda that links innovation with trust, openness with safeguards, and cooperation with capacity building.

APEC 2026 offers a timely opportunity to frame inclusive digital governance as a core pathway toward shared prosperity. The region does not need a single legal model. It needs shared direction, practical tools, interoperable standards, and sustained collaboration. In this sense, the task is not only to build smarter economies, but to build more inclusive AI communities.

To prosper together, the Asia-Pacific must govern together.

15. National Institute of Standards and Technology, Artificial Intelligence Risk Management Framework: Generative Artificial Intelligence Profile, NIST AI 600-1 (Gaithersburg, MD: National Institute of Standards and Technology, July 2024), 1–4, 11–13, 26, 29–31, accessed May 27, 2026, https://doi.org/10.6028/NIST.AI.600-1.

The CBPR Model for Harmonizing Digital Governance Regimes: From the APEC to the Global

Yueh-Ping (Alex) YANG

Associate Professor, National Taiwan University College of Law. Co-Chair, WTO Chair Programme (Phase III). Secretary, Society of International Economic Law. Director, Asian Center for WTO & International Health Law and Policy. S.J.D. Harvard Law School. The author can be reached at alexypyang@ntu.edu.tw.

I.Digital Governance in Divergence in the Three Kingdom Era

Commentators have observed that the world's digital governance regimes feature the "Three Digital Kingdoms" landscape: the European Union ("EU"), China, and the United States.[1]

The EU adopts a privacy- and consumer-oriented model. The General Data Protection Regulation ("GDPR"), Digital Services Act ("DSA"), Digital Markets Act ("DMA"), and Artificial Intelligence Act ("AI Act"), among others, have introduced layers of regulations aiming at protecting consumers' welfare, including privacy, safety, transparency, fairness, and human dignity. These regulations, famous for their "Brussels Effect,"[2] effectively restrict foreign digital services and serve the EU's industrial interest and digital sovereignty.

China also takes a heavy hand in the digital market, but less for consumer welfare than national security. A notable instance is its data outflow restrictions, which require not only the data subject's informed consent but also the approval of the data outflow security assessment conducted by the national cyberspace information authorities.[3] This security-oriented attitude inevitably entails greater state intervention in data governance, aligning with China's political priority of national security and state control.

The United States, as the world's largest exporter of digital services, has traditionally held a liberal view on data governance, prioritizing free data flow and less market regulation. However, it seems to have taken a step back recently, as evidenced by its stance against TikTok, among other things. This recent change coincides with its industrial relations, particularly with China. Due to China's cyber controls, the United

1.See, generally ANU BRADFORD, DIGITAL EMPIRES: THE GLOBAL BATTLE TO REGULATE TECHNOLOGY (2023).
2.See generally ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD (2020).
3.DATA OUTFLOW SECURITY ASSESSMENT REGULATION (数据出境安全评估办法), art. 4 (China).

States' internet giants, e.g., Amazon, Google, and Facebook, have limited, if any, access to China's market, while China's counterparts, e.g., TikTok and SHEIN, are free to operate in the United States and have reached tremendous success. This imbalance undeniably places the United States at a disadvantage, which might explain its shift.

In a nutshell, these Three Kingdoms possess divergent digital governance models due to differences in industrial structures, consumer protection commitments, privacy protection levels, national policies, and more. These vast gaps render it challenging to harmonize at a state-to-state level.

II.Harmonization Efforts, but in Vain

Different digital governance regimes inevitably conflict, necessitating harmonization. Examples include the unilateral, bilateral, and even multilateral approaches.

As a default approach, each country could unilaterally impose its digital governance laws on other countries. Essentially, this is an exercise of its sovereignty over the regulation of digital markets within its jurisdiction. Foreign digital service providers inevitably must comply with the domestic game rules when conducting business in domestic markets. The apparent impact of this unilateral approach is that each country's data laws will apply cumulatively to multinational digital service providers, thereby increasing their compliance costs. Sometimes the restrictions could be so prohibitive that foreign digital service providers would be unable to enter the market. Digital services will then become more costly and restrictive, resulting in less efficient resource deployment for developing digital markets and potential protectionism.

Given the apparent shortcomings of the unilateral approach, many regional trade agreements have begun coordinating their members' digital governance regimes through bilateral channels. Famous mega-free trade agreements, e.g., the Comprehensive and Progressive Agreement for Trans-Pacific Partnership ("CPTPP") and the Regional Comprehensive Economic Partnership ("RCEP"), contain electronic commerce chapters to harmonize digital governance regimes.

Another notable bilateral attempt is the Digital Economy Partnership Agreement ("DEPA"), widely regarded as a breakthrough in international digital law. Notably, DEPA highlights mechanisms for harmonizing Parties' digital governance regimes, particularly the privacy protection frameworks. For instance, it enumerates the harmonization mechanisms, including the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement; broader international frameworks; appropriate recognition of comparable protections afforded by their respective legal frameworks' national trustmark or certification frameworks; or other avenues for the transfer of personal information between the Parties.

Even multilateral negotiations have witnessed some progress. At the 14th WTO Ministerial Conference in March 2026, 66 WTO Members adopted the Agreement on E-Commerce with Interim Arrangements, marking a milestone toward multilateral rules to harmonize digital governance regimes among WTO Members.[4]

4.WTO, Members Adopt a Pathway to Bring E-Commerce Agreement into Force via Interim Arrangements, https://www.wto.org/english/news_e/news26_e/mc14_28mar26_341_e.htm (last visited June 2, 2026).

Despite various attempts to harmonize digital governance regimes across jurisdictions, achievements at the state-to-state level appear limited. In cases that reach some progress, progress remains limited, if any. Mostly, they adopt relatively abstract and principle-based terms to harmonize digital governance regimes and reduce trade restrictions. However, they also provide ample room for exceptions based on abstract terms, such as legitimate public policy objectives. Therefore, they can hardly prevent certain countries, such as the EU or China, from regulating foreign digital services operating in their markets on the basis of personal data, national security, or other public concerns.

III.From the APEC to Global: The Novel CBPR Model

Among the various parallel efforts to harmonize different digital governance regimes, I notice a novel approach emerging from the APEC: the Cross-Border Privacy Rules ("CBPR") System. I view this CBPR Model as having the potential to drive further harmonization, and I believe it deserves more attention from global policymakers.

APEC's CBPR System addresses the cross-border data transfer issue, a crucial topic for data governance regimes. It originated from APEC's Privacy Framework, setting out nine principles to ensure information privacy. In 2011, APEC Leaders endorsed APEC's CPBR System, a voluntary and accountability-based system that facilitates privacy-respecting data flows among APEC economies. It recognizes the difficulties in achieving consensus among members and therefore provides a more flexible "certification system" aimed at "organizations," helping them demonstrate compliance with the privacy principles laid out in the APEC Privacy Framework by participating in the system.

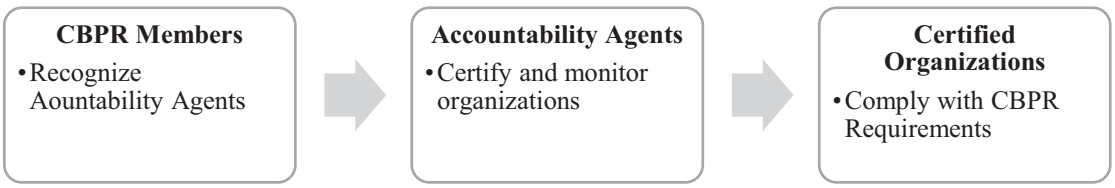
APEC's CBPR System also makes clear that it imposes no obligations on APEC economies or non-participating governmental agencies.[5] APEC economies may determine whether to join this system voluntarily. As of May 2026, 9 economies have participated in APEC's CBPR system, i.e., the United States, Mexico, Japan, Canada, Singapore, the Republic of Korea, Australia, Chinese Taipei, and the Philippines.[6]

In 2022, some participating economies announced the Global Cross-Border Privacy Rules Declaration, which extends the CBPR rules beyond APEC economies and establishes the Global CBPR Forum. As of May 2026, the Global CBPR Forum has 10 members, including Australia, Canada, Dubai International Finance Centre, Japan, the Republic of Korea, Mexico, the Philippines, Singapore, Chinese Taipei, and the United States, and 4 associates, including Bermuda, Nigeria, Mauritius, and the United Kingdom.[7]

CBPR's main feature is the introduction of a data privacy certification system aimed at "organizations" rather than "states." It introduces a government-backed certification system at a global level. Organizations may obtain certification by adhering to CBPR's privacy protection standards, thereby demonstrating compliance with globally recognized data privacy standards. The certification, in turn, may serve as a basis for these organizations to earn the public's trust and thus

5.CHARTER OF THE APEC CROSS-BORDER PRIVACY RULES AND PRIVACY RECOGNITION FOR PROCESSORS SYSTEMS JOINT OVERSIGHT PANEL, art. 1.1(i) and (iv).
6.CBPR, Government, https://cbprs.org/government/ (last visited June 2, 2026).
7.Global CBPR Forum, Members & Associates, https://www.globalcbpr.org/about/membership/ (last visited June 2, 2026).

Chart 1: The Overview of the CBPR Model



facilitate data transfer among CBPR members with fewer legal obstacles.

At the core of CBPR are the Accountability Agents ("AAs"). AAs are the certification bodies recognized by the Global CBPR Forum to certify organizations' privacy protection practices, which can be private entities or governmental agencies. AAs will evaluate whether to award the certification in accordance with the related CBPR Requirements. They will further conduct ongoing monitoring and compliance review processes of the certified organizations. They may further impose penalties against noncompliant organizations.

AAs are, in turn, scrutinized by the Global CBPR Forum. In conducting their certification, AAs must comply with the Recognition Criteria designed by the Global CBPR Forum. Moreover, AAs must obtain recognition from the Global CBPR Forum. Therefore, AAs are not purely private certification bodies but certification bodies backed by CBPR members.

In sum, the CBPR Model features a delegated two-tier model for facilitating cross-border data transfer between members. In the first tier, CBPR members recognize AAs and agree on the general principles or guidance for AAs to conduct certification. In the second tier, AAs certify the organizations and monitor their compliance with CBPR requirements. The relationship between CBPR members, accountability agents, and certified organizations may be described as follows:

As of May 2026, the Global CBPR Forum has recognized 9 AAs.[8] These AAs have, in turn, certified 130 participating organizations.[9] Overall, the CBPR Model has achieved some progress.

IV. Reflections on the CBPR Model Extensions

As a novel approach to harmonizing digital governance regimes, the CBPR Model has three key features worth highlighting: its soft-law nature, the public-private gatekeeper model, and a bottom-up approach.

First, CBPR adopts a soft-law approach to facilitate cross-border data transfer, in which countries may voluntarily decide whether to participate in CBPR and how to formulate their domestic laws on cross-border data transfer. This soft-law approach aims to maximize global adoption of CBPR.

Second, CBPR's real harmonization effort targets the "standards" and "gatekeepers" that organizations use to conduct cross-border data transfers, not the "laws" and "countries." In practice, private certification bodies, such as the International

8.Global CBPR Forum, Accountability Agents, https://www.globalcbpr.org/accountability-agents/ (last visited June 2, 2026).
9.Global CBPR Forum, Certified Organizations, https://www.globalcbpr.org/privacy-certifications/directory/ (last visited June 2, 2026).

Organization for Standardization ("ISO"), play an influential role in developing and enforcing internal controls for data privacy and security. CBPR injects more public elements into the existing private gatekeeper model by introducing a recognition system for these certification bodies, i.e., the AAs, thereby escalating it to a "public-private gatekeeper model." Moreover, this recognition regime bears a global nature, recognized not only by a single country but by all CBPR members.

Third, by promoting more common data management standards and practices among members, CBPR envisages a bottom-up approach that may drive the convergence of data legislation in the future. Several members have adopted legislation that admits cross-border data transfer based on the CBPR certification, such as Japan and Singapore. These cases demonstrate the potential of CBPR's bottom-up approach. If CBPR's certification gains voluntary recognition from more members, it may effectively serve as a single pass for cross-border data transfer. In that case, cross-border data transfer may be facilitated in accordance with CBPR standards and certification, despite divergent data laws among members.

Admittedly, the CBPR Model is far from being perfect. It still needs to increase its global adoption, promote more voluntary recognition, and better enforce its data protection commitments. That said, it has laid a foundation with sound rationale to foster cross-border data transfer, and this rationale has the potential to be extended elsewhere to harmonize digital governance regimes.

V.Concluding Remark

Harmonizing digital governance regimes is never an easy task and requires creativity. In this comment, I introduce the novel CBPR Model, which takes a different state-to-gatekeeper approach that creates a global recognition and certification system. It introduces a more inclusive, practical, and less interventionist approach to coordinating cross-border data transfer certification standards at the gatekeeper level. It also adopts a bottom-up approach to promote recognition at the state level and creates a single pass in the long run. While CBPR's future success remains to be seen, its design rationales warrant further attention from global policymakers.

Healthcare AI After COMPUTEX and WHA79: From Infrastructure Momentum to Governance Readiness

Frances Chang
M.A, ABAC Secretariat

The healthcare AI debate is entering a more practical stage. For the Asia-Pacific, the next policy question is no longer whether AI can support health systems. That answer is already clear enough. The harder question is how AI can move from infrastructure, pilots and corporate showcases into health systems in ways that are clinically useful, locally adaptable and publicly trusted. Developments observed from late May to early June, around COMPUTEX 2026 in Taipei and the 79th World Health Assembly, offer two useful windows into this shift.

Around COMPUTEX 2026, Taiwan's technology firms are now positioned deeper inside the global AI infrastructure cycle. The attention around NVIDIA's Vera Rubin platform and its production ramp through Taiwan's server makers and supply chain partners reflects a broader shift. Taiwan has moved beyond supplying parts of the AI boom; its firms are increasingly involved in the systems through which AI becomes deployable, including servers, cooling, networking, edge devices, data centre build-out and system integration. This infrastructure momentum gives firms more room to move into application layers. It also creates pressure to find higher-value sectors where AI capability can become a sustainable business. Healthcare is one of the most consequential frontiers for this transition.

This is already visible in the direction of corporate activity. Smart hospitals, medical edge devices, physical AI, AI-assisted workflows and health data platforms are becoming part of the business imagination around AI. For Taiwan's ICT firms, healthcare offers both market potential and strategic relevance. Ageing societies, workforce shortages and rising care costs create demand for tools that can support diagnosis, hospital management, rehabilitation, remote care and precision medicine. Yet healthcare also carries a higher burden of proof than most AI applications. A model or platform cannot rely on technical performance alone. It must fit clinical workflows, meet regulatory expectations and earn trust from institutions and users. The move from AI infrastructure to healthcare application therefore brings business opportunity and governance pressure together.

At the global health governance level, discussions around WHA79 pointed in the same direction. The Assembly did not treat AI simply as a general digital health issue. Its discussions placed AI and data-driven innovation inside concrete health-system functions, including precision medicine, pharmacovigilance and teleradiology. The resolution on precision medicine

emphasised the use of clinical, molecular, genomic and other health data, while also highlighting the need for infrastructure, workforce capacity, governance, affordability and inclusive data systems. The discussion on smart pharmacovigilance strengthened the case for safety monitoring, real-world data and regulatory capacity. Teleradiology linked digital health and AI to remote diagnostics, medical imaging, patient safety and clinical oversight.

These signals matter because they show where healthcare AI governance is heading. The debate is becoming more specific. AI is no longer floating above health policy as an abstract innovation. It is being attached to the functions that health systems already need to govern: diagnosis, monitoring, treatment selection, safety surveillance and service delivery. This creates a clearer regulatory agenda. Governments will need to ask how AI tools are validated before use, monitored after deployment, updated over time and adapted to local populations. Health systems will need the capacity to judge when AI is useful, when it is excessive and when simpler tools may serve patients better.

Recent research in digital health reinforces this turn[1]. One emerging concern is the gap between model scale and clinical value. Large-scale AI models, especially generative AI and foundation models, require substantial data, storage and compute resources. The issue is not only environmental cost. Large-scale AI in healthcare remains unclear compared with task-specific methods, and that healthcare AI development should define expected patient outcomes and resource costs from the outset. This points to a sharper governance principle: healthcare AI should be assessed by fitness for purpose, not by model size or novelty.

AI outputs should serve as starting points for exploration, validation and refinement[2]. Human expertise remains central to judgement, contextual interpretation and responsibility. This has direct governance implications. Simply keeping humans "in the loop" is too vague. Health systems must define who reviews AI outputs, what training they need, how model versions and prompts are recorded, how errors are managed and how accountability is assigned. AI literacy becomes part of health system readiness.

For the Asia-Pacific, this readiness question is decisive. The more important divide will be between health systems that can validate, govern and adapt AI tools, and those that must import them as black-box solutions. Healthcare AI will reproduce existing inequalities if economies lack data quality, clinical validation capacity, procurement rules, cybersecurity safeguards, trained users and regulatory expertise.

Business innovation can help identify these gaps early. Firms trying to deploy healthcare AI will quickly encounter practical barriers: unclear medical device classification, fragmented data rules, uneven hospital readiness, uncertain liability, and weak cross-border validation mechanisms. These barriers are governance signals. They show where policy must become more concrete.

Healthcare AI will grow because firms now have the infrastructure, incentives and technical capacity to build it. COMPUTEX showed the business momentum behind that shift. WHA79 showed the health-system functions where governance expectations are becoming more concrete. The policy task is to connect these two developments before deployment outruns trust. Good governance will decide which forms of healthcare AI are worth scaling, under what conditions, and for whose benefit.

1.Raghavendra Selvan, "Sustainability of large-scale artificial intelligence models in health care", The Lancet Digital Health, 2026.
2.Ariel Yuhan Ong et al., "Co-intelligence: a proposal for human-artificial intelligence collaboration for large language models in medical research", The Lancet Digital Health, 2026.

CTPECC

Chinese Taipei Pacific Economic Cooperation Committee

Published in March 2026

5th Floor, Number 16-8, Dehuei Street,
Zhongshan District, Taipei City 10461,
Taiwan (Republic of China)

Website

Reader Survey

For more information,
Please visit CTPECC website or email d35110@tier.org.tw, d23320@tier.org.tw

Authors of Asia-Pacific Perspectives should assure that they have cited references accurately in their articles and take the responsibility individually.
This publication is made of environmentally friendly paper.