Workshop on Privacy Enhancing Technologies

Opportunities and Challenges

APEC Digital Economy Steering Group

February 2026

Asia-Pacific
Economic Cooperation

Asia-Pacific
Economic Cooperation

Workshop on Privacy Enhancing Technologies

Opportunities and Challenges

APEC Digital Economy Steering Group

February 2026

APEC Project: DESG 103 2024A

Produced by
Yu-Hong QUE & Peggy KAO, Project Overseer
Ministry of Digital Affairs, Chinese Taipei

With support of:
APEC Digital Economy Steering Group
National Institute of Cyber Security

For
Asia-Pacific Economic Cooperation Secretariat
35 Heng Mui Keng Terrace
Singapore 119616
Tel: (65) 68919 600
Fax: (65) 68919 690
Email: info@apec.org
Website: www.apec.org

APEC#226-CT-04.2

The terms such as “national”, “nation” used in the text are for purposes of this report and do not imply the “political status” of any APEC member economy.

Contents

1. Introduction

This project summary report is an output of an APEC-ASF Digital Innovation Sub-Fund project under the Digital Economy Steering Group (DESG), “DESG_103_2024A — Workshop on Privacy-Enhancing Technologies: Opportunities and Challenges.” It is co-sponsored by Australia; Chile; Japan; the Republic of Korea; and the United States.

In today’s digital era, where data is a critical driver of economic development across APEC economies, balancing data use with privacy protection remains a significant challenge. Emerging Privacy-Enhancing Technologies (PETs)—including Differential Privacy, Synthetic Data, Federated Learning, and Homomorphic Encryption—are proving to be promising tools that support secure data sharing, collaboration, and compliance with data protection regulations. As APEC economies undergo digital transformation, these technologies can foster innovation, trust, and economic integration, particularly for cross-border data flows. However, despite their potential, PETs also present risks and implementation challenges that must be carefully managed.

Chinese Taipei proposes this project to provide APEC economies with a platform to share and discuss PETs. The project seeks to raise awareness, exchange experiences, highlight policy considerations, and identify areas for future cooperation.

This project convenes a workshop for policymakers, regulators, technical experts, and private-sector representatives. The physical workshop was held on 12 September 2025. In addition to the keynote speech, the one-day program comprised three plenary sessions: Policy and Institutional Design, Technological Innovation, and Practical Application.

There were 99 participants from 11 economies, including Canada; Chile; Indonesia; Japan; Mexico; Papua New Guinea; the Philippines; Singapore; Chinese Taipei; Thailand; and Viet Nam, as well as non-member participants from Belgium.

2. Topic-Based Summaries of Presentations

2.1 Keynote Speech – Enabling Trust, Empowering Growth: The Strategic Role of PETs in Modern Data Governance

Ms. Natascha Gerlach, Director of Privacy Policy at the Centre for Information Policy Leadership (CIPL), Belgium, delivered a keynote address on the transformative role of Privacy-Enhancing Technologies (PETs) in advancing responsible data use and AI innovation. She emphasized that PETs represent the technical embodiment of accountability, allowing data to be used while preserving individual privacy and data security.

1. CIPL's Role and the Importance of PETs

For almost 25 years, CIPL has operated as a global data policy think tank, focusing on thought leadership regarding accountable data practices to unlock the potential of data—the "fuel for our digital economies"—in a rights-preserving manner. PETs are critically recognized by companies, governments, and regulators as technical tools essential not only for protecting valuable data assets but also for actively making use of them. CIPL views PETs as the technical expression of accountability and the responsible use of data. This topic is timely, as PETs have steadily gained attention for integrating privacy, security, and confidentiality into the design and architecture of technology-based solutions. CIPL has significantly contributed to the discourse with two key papers: one published in 2023 reflecting on the PETs landscape and adoption incentives, and the second one released earlier in 2024 specifically examining PETs in the context of Artificial Intelligence (AI).

2. Defining and Categorizing PETs

CIPL defines PETs (or Privacy-Preserving Technologies, PPTs) as technical means that facilitate the processing and use of data in a way that preserves individual privacy and data security while maintaining its informational value. This definition emphasizes the continued utility of data, distinguishing them from simple encryption which may render data unusable at the source.

PETs are categorized into three main groups:

- Cryptographic Tools: Advanced techniques where certain data elements remain hidden even while in use. Examples include Homomorphic Encryption (HE), Secure Multi-Party Computation (SMPC), Trusted Execution Environments (TEEs), and Zero-Knowledge Proofs (ZKPs).
- Distributed Analytics Tools: Technologies that process data at its source to avoid centralized collection. A prime example is Federated Learning (FL).
- Obfuscation Tools: Solutions that limit or entirely remove the potential for individual identification from data. Key technologies include

Differential Privacy (DP) and Synthetic Data.

3. The Value Proposition: Compliance and AI

Despite the complexity, resource intensity, and need for specialized experts, PETs are critical tools for several compelling reasons.

Supporting Privacy Compliance

PETs predominantly support general privacy compliance. They assist with common data protection principles:

- Secure Data Processing: Technologies like HE, SMPC, TEEs, and FL keep data hidden during use and reduce the risk of unauthorized access.
- Data Minimization and Purpose Limitation: ZKPs, SMPC, and FL limit data visibility and access to what is strictly necessary for a given purpose.
- Anonymization and Pseudonymization: DP or synthetic data can limit or entirely remove the potential for identifying individuals, effectively making the data non-personal.
- Cross-Border Data Flows: In jurisdictions with restrictions on data transfers, FL and SMPC can facilitate computation without the raw data physically crossing borders.
- Demonstrating Accountability: PETs support organizations in demonstrating accountability and privacy by design.

Application in the AI Life Cycle

PETs are increasingly embedded into every stage of AI development and deployment.

- Data Generation: Synthetic data has emerged as a potential alternative when real data is scarce or too sensitive.
- Model Training: Homomorphic encryption allows models to be trained directly on encrypted data. Differential Privacy injects statistical noise into data sets or model updates. Federated learning allows multiple organizations or devices to train a shared model without the data leaving its source.
- Future AI: The role PETs must play in new developments, such as Agentic AI (which executes complex, adaptive tasks autonomously), is obvious, and CIPL is currently researching this topic.

4. Trade-offs and Barriers to Adoption

PETs are not a "silver bullet" for all privacy challenges; each technology presents inherent complexities and trade-offs that require careful consideration.

Technical Trade-offs

The primary tension is between privacy and utility.

- Synthetic Data: Risks include replicating bias inherent in real data, re-identification, or inference attacks.
- Homomorphic Encryption: The computational costs can be very high, and careful implementation is necessary to maintain model performance.
- Secure Multi-Party Computation: Incurs high communication costs, leading to scalability challenges, and carries collusion risk.
- Differential Privacy: Requires finding the right balance for noise and data accuracy; too much noise renders data unusable, while too little leaves privacy risks.

Organizational and Policy Hurdles

Adoption faces significant hurdles, which differ across organizational size and industry:

- Complexity and Integration: PETs are not standalone solutions and often require custom implementation, making integration into existing workflows challenging. They are not yet "plug and play".
- Lack of Standards and Metrics: The absence of universally agreed-upon standards and regulatory frameworks hinders the ability to measure PET effectiveness, assess risk mitigation potential, and determine Return on Investment (ROI), making it difficult to get board-level buy-in.
- Cost and Resources: PETs can be expensive, posing a serious challenge for Small and Medium-sized Enterprises (SMEs).
- Knowledge Gap: Many companies lack sufficient internal knowledge and expertise about PETs.

Regulatory Challenges

Regulators also face key hurdles, including a lack of awareness, expertise, and resources needed to build specialized capacity to test and oversee complex PET solutions. The PET ecosystem is still evolving, and while regulatory sandboxes are effective tools, they are resource-intensive. Furthermore, without a common definition, developing standard benchmarks to assess the appropriate privacy-utility trade-offs remains a challenge.

5. Global Regulatory Shift and Roadmap

Despite the challenges, governments and regulators worldwide are driving PET adoption with concrete actions, signaling a major shift in technological governance. For example, Singapore's Infocomm Media Development Authority (IMDA) described PETs as a "superpower" and launched a sandbox. The UK’s ICO now views PETs as a regulatory expectation essential for GDPR obligations.

To accelerate the use of PETs, the community should follow six key priorities:

- Raise Awareness and build capacity: Proactive efforts, such as webinars and accessible educational materials, are needed.
- Develop Standards and Best Practices: International bodies should work on creating PET standards and certification frameworks.
- Enhance Regulatory Clarity: Regulators must collaborate to provide consistent guidance, develop regulatory sandboxes, and create toolkits especially useful for smaller organizations.
- Support Innovation and Market Development: Industry, academia, and startups should jointly promote research, development, and pilot projects to mature PET solutions for easier organizational adoption.
- Address Cost and Resource Constraints: Companies should view PETs as an investment in security that unlocks valuable data assets, rather than an isolated expense. Developers can assist by offering open-source PET tools.
- Shift Mindset: Privacy professionals must evolve from simply citing the law to becoming responsible use enablers who understand technology and business drivers. Regulators must shift from an enforcement mindset to becoming active partners by providing incentives (e.g., considering the use of PETs positively in enforcement decisions).

2.2 Plenary I: Policy and Institutional Design

Below is a summary of the main points from the presentation *Canada's Role in Advancing Policy Pathways for PETs*:

Ms. Runa Angus, Senior Director of Innovation, Science and Economic Development (ISED), Canada, delivered an overview of Canada's domestic and international efforts to promote PETs as tools to strengthen digital trust and enable responsible data innovation. Speaking from both her role at ISED and as Chair of the Organization for Economic Co-operation and Development (OECD) Working Party on Data Governance and Privacy, she emphasized that PETs are vital to reconciling privacy protection with the needs of AI development and global data flows.

1. Background: Building Trust in the Digital Economy

- Canada's economic prosperity is heavily tied to international trade—exports and imports exceeded CAD 2 trillion in 2024, accounting for about two-thirds of the economy's GDP, and one in five Canadian jobs depends on exports.
- The digital economy represents a fast-growing share, with data-related investments increasing tenfold since 1990 and over 12% of Canadian businesses now using AI, double the figure from the previous year.
- However, public concern about privacy remains high: 93% of Canadians express concern over data protection, while only 33% believe AI will positively impact the economy.
- Ms. Angus stressed that trust is the cornerstone of digital adoption, and robust privacy frameworks are no longer mere compliance tools but competitive advantages in global trade.

2. Canada's Domestic and International Frameworks

- Domestically, Canada's Personal Information Protection and Electronic Documents Act (PIPEDA, 2000) provides a foundation for private-sector data governance, built on principles of accountability, meaningful consent, and safeguards for data quality and retention.
- The Act requires organizations to ensure equivalent protection when transferring data across borders, maintaining a high standard of privacy even when third parties process information abroad.
- Internationally, Canada actively advances interoperability across privacy regimes. Key initiatives include:
  (1) Leadership in the OECD privacy guidelines and the Declaration on Trusted Government Access to Personal Data.
  (2) Endorsement of Data Free Flow with Trust (DFFT)—originally

initiated by Japan—and reaffirmed under the G7 2025 Leaders' Statement on AI for Prosperity.

(3) Engagement with APEC, the United Nation Working Group on Data Governance, and the Canada–EU Digital Partnership, alongside domestic consultations on Cross-Border Privacy Rules (CBPR) and Privacy Recognition for Processors (PRP) systems.

3. The Role of PETs in Canada's Data Strategy

- PETs are viewed as key enablers that balance innovation with privacy protection, particularly in sensitive sectors such as healthcare and finance.
- Examples include:

  (1) Synthetic data and differential privacy for secure AI model training and fraud detection.

  (2) Federated learning to enable cross-border AI collaboration without exposing raw data.

  (3) Trusted execution environments for secure computation of financial and health data.
- PETs support data minimization, confidentiality, and responsible AI deployment, complementing legal frameworks and enhancing cross-border trust.

4. International Collaboration: OECD PETs and AI Workshop

- Canada co-hosted the 3rd OECD Expert Workshop and High-Level Roundtable on PETs and AI (June 16–17, 2025, Ottawa) with the Digital Agency of Japan and the OECD, following earlier sessions in the UK–Estonia and Singapore.
- The two-day event brought together 70 in-person and 40 virtual participants from governments, data protection authorities, academia, and the private sector.
  - Day 1 (Technical focus): Showcased case studies demonstrating how PETs enable secure medical research, AI-based fraud detection, and data analytics while preserving confidentiality.
  - Day 2 (Policy focus): Addressed barriers such as fragmented regulatory frameworks, lack of standards, and unclear market incentives. Participants called for stronger policy signals that PETs are not just promising tools but strategic enablers of the next frontier of data innovation.

5. Key Takeaways and Next Steps from Canada's experience

- Policy Alignment: Greater international coordination and regulatory clarity are critical to scale PETs across sectors and jurisdictions.
- Global Repository: OECD is leading work on a global repository of PETs use cases to share practices and improve comparability.
- Ecosystem Approach: OECD Workshop participants endorsed forming a cross-sector PET network linking policymakers, regulators, academia, and industry.
- Certification and Safe Harbors: Independent certification frameworks and regulatory safe harbors were suggested to incentivize PET adoption and reduce compliance uncertainty.
- G7 Integration: Canada intends to incorporate these findings into its G7 digital and technology agenda, advancing international cooperation on PETs.

6. Conclusion

Ms. Angus concluded by recognizing the OECD's leadership in shaping global PET policy through two major reports—Emerging Privacy-Enhancing Technologies: Current Regulatory and Policy Approaches (2023) and Sharing Trustworthy AI Models with PETs (2025)—and the forthcoming global repository initiative. She affirmed that while PETs are not a cure-all for privacy or innovation challenges, their potential to foster trust, security, and responsible data use is already evident. Achieving this vision, she noted, will require sustained international collaboration to align policy frameworks and unlock the economic and societal value of trusted data flows.

Below is a summary of the main points from the presentation *Why PETs Potentially Redesign the Discourse of Traditional Regulatory Framework*:

Mr. Kohei Kurihara, CEO of Privacy by Design Lab, Japan, explored how PETs may reshape the way societies design and implement privacy regulations in the AI era. Drawing on his organization's experience promoting privacy culture and stakeholder collaboration since 2020, he argued that PETs are more than technical tools—they represent a paradigm shift toward participatory and preventive governance.

1. Revisiting the Roots: Privacy by Design and Its Evolution

Mr. Kurihara began by tracing the origins of Privacy by Design (PbD), a framework introduced by Dr. Ann Cavoukian in the 1990s during the commercialization of the Internet.

- PbD established seven foundational principles, emphasizing proactive—

not reactive—measures, privacy as the default, and full functionality (a *positive-sum* rather than *zero-sum* approach).

- Mr. Kurihara noted that these ideas anticipated the rise of large-scale networked data systems and today's AI ecosystems, where end-to-end security and user-centric design remain critical.
- He highlighted that PbD now extends beyond IT systems to include business practices and physical infrastructure, forming a *"trilogy"* that embeds privacy across the entire data lifecycle.

2. Modernizing Regulation: From Rules to Design

Building on PbD, Mr. Kurihara discussed how global policy frameworks are moving toward a "by design, by default" model, as codified in Article 25 of the EU GDPR.

- He cited the OECD's data governance model, which links regulation, infrastructure, and leadership capacity into a coherent data value cycle.
- In an era of AI-driven automation, he argued that traditional rule-based regulation can no longer operate in isolation; it must integrate technical safeguards and dynamic collaboration among sectors.
- PETs play a central role in this modernization—embedding privacy into digital infrastructure itself, rather than treating compliance as an afterthought.

3. PETs as a Bridge Between Technology and Ethics

Mr. Kurihara explained that PETs embody the technical realization of PbD principles, ensuring that data minimization, pseudonymization, and confidentiality are achieved at the system level.

- He illustrated this with examples such as encrypted messaging, federated AI model training, and privacy-preserving fraud detection.
- PETs, he argued, are not just "add-ons" for compliance but foundational components of trustworthy digital infrastructure, capable of mitigating risks from government surveillance, data misuse, and AI inference attacks.

4. Multi-Stakeholder Collaboration and the "Stakeholder Theory"

In the latter part of his talk, Mr. Kurihara applied Professor R. Edward Freeman's Stakeholder Theory to privacy governance, arguing that trust must be co-created by all parties—governments, companies, and consumers.

- Consumers, he noted, value convenience and personalization; according to research by Kantar and Google, over 80% find targeted ads occasionally useful, and a positive privacy experience can boost brand preference by 43%.

- Businesses view PETs as strategic investments: reports from International Association of Privacy Professionals (IAPP) and Cisco show that over 80–90% of privacy professionals have expanded responsibilities related to privacy governance.
- Governments increasingly endorse PET adoption through policy statements such as the 2025 G7 Data Protection Authorities' Communiqué and Global Privacy Assembly resolutions, which urge privacy-preserving innovation and capacity building.

Mr. Kurihara concluded that the future regulatory environment should shift from a top-down, rule-imposing model to a collaborative, PETs-enabled ecosystem, where all stakeholders share responsibility for trustworthy data use.

5. Conclusion

Mr. Kurihara closed by urging a rethinking of the regulatory ecosystem as AI and data technologies continue to evolve. Just as privacy frameworks emerged during the commercialization of the Internet in the 1990s, the AI era now calls for co-governance models integrating PETs into both design and policy.

He envisioned PETs not merely as compliance tools, but as social infrastructures that sustain transparency, user trust, and innovation. By embedding privacy into the architecture of emerging technologies, societies can ensure that the next generation of digital regulation is preventive, inclusive, and human-centric.

Key Takeaways from Plenary I Panel Discussion

This panel discussion featured Ms. Runa Angus (Canada) and Mr. Kohei Kurihara (Japan), moderated by Dr. Chin-Li Wang (Chinese Taipei), focusing on the intersection of privacy policy, technology governance, and the global development of Privacy-Enhancing Technologies (PETs). The exchange explored how governments can create effective policy signals, the value of technology-neutral regulation, and the role of international cooperation mechanisms such as APEC CBPR in promoting trust and interoperability.

1. Policy Signals and Practical Incentives for PETs

Ms. Angus highlighted that while technical challenges in PETs can be addressed, policy uncertainty remains the greater barrier. Policymakers should focus on incentivizing adoption rather than mandating use. She outlined three key approaches:

- Legislative Clarity: Laws should clearly define what constitutes PETs and explicitly state that privacy legislation does not apply to anonymized data. Such clarity immediately encourages technological deployment.
- Regulatory Sandboxes: These allow organizations to test compliance strategies under the guidance of Data Protection Authorities (DPAs), fostering innovation through one-on-one regulatory support.
- Incentives and Liability Reduction: Certification systems and sandbox participation can offer liability reduction and reputational advantages to companies adopting verified PETs.

2. Integrating "Security by Design" and "Privacy by Design"

Mr. Kurihara emphasized that security and privacy must coexist and cannot be treated as separate domains.

A "by design" approach requires integrating PETs and privacy measures early in product development. Compromised privacy inevitably undermines product safety. He urged collaboration between privacy and security professionals, especially given rising domestic security concerns, to ensure technologies are safe for users and do not create systemic risks.

3. Institutional Roles and Multi-Stakeholder Collaboration

In response to whether the Auditor General of Canada (AG) plays a role in promoting PETs, Ms. Angus clarified that the AG does not hold a formal position. Instead, PETs advancement is driven by multi-stakeholder coordination among the Department of Innovation, Science and Economic Development (ISED), the Office of the Privacy Commissioner, the OECD, and international partners. This collaborative model reflects Canada's approach to building policy legitimacy and regulatory coherence.

4. Technology-Neutral Regulation and Future-Proof Policy

Ms. Angus argued that Canada's principles-based and technology-neutral framework under the Personal Information Protection and Electronic Documents Act (PIPEDA, 2000) remains effective because it provides flexibility amid rapid technological change.

- Such neutrality allows policymakers to adapt through guidelines and interpretive codes rather than frequent legislative amendments.
- She underscored that since lawmaking is slow, getting the foundational principles right from the outset is crucial for sustainability.

Mr. Kurihara added that as PETs evolve alongside new inventions, continuous stakeholder involvement is vital for checks and balances. He warned that while governments may sometimes intervene to prevent harms, overregulation could be perceived as weakening privacy. Therefore, democratic oversight is necessary to ensure PETs remain a policy priority and do not become sidelined under domestic or economic security narratives.

5. Cross-Border Governance and the Role of APEC CBPR

Both speakers addressed how international cooperation frameworks like APEC's CBPR can facilitate PETs adoption and regulatory alignment.

- From Canada's Perspective: Ms. Angus noted that Canada is in the process of consulting on CBPR adoption. She viewed the framework as a trust-building mechanism that helps companies manage cross-border risk by ensuring that certified organizations meet comparable privacy standards. While CBPR does not replace domestic compliance, it provides a competitive advantage for certified firms. She also observed that growing attention to data sovereignty in Canada has increased scrutiny of cross-border data flows, making CBPR-type mechanisms timely and relevant.
- From Japan's Perspective: Mr. Kurihara identified three key drivers for successful certification:

  (1) Legal Cost: Firms handling multi-economy data transfers face heavy compliance burdens that CBPR can help streamline.

  (2) Incentive: Governments should provide tangible business incentives to encourage participation, rather than merely imposing approvals.

  (3) Opportunity: CBPR should be framed as an *enabler* of cross-border business growth, supported by active diplomatic cooperation between jurisdictions such as Canada and Japan.

2.3 Plenary II: Technological Innovation

Below is a summary of the main points from the presentation *Challenges in Implementing Privacy Compliance Automation Technology (PCAT) in Thailand*:

Mr. Pakorn Thongjeen, CEO of Security Pitch, Thailand, shared Thailand's six-year journey implementing the Personal Data Protection Act (PDPA) and developing Privacy Compliance Automation Technology (PCAT). Speaking as a practitioner rather than an academic, he outlined how his company, Security Pitch, became the economy's first developer of integrated privacy and cybersecurity automation systems to operationalize PDPA compliance.

1. Thailand's PDPA Implementation Journey

- PDPA Enactment and Enforcement: Thailand's PDPA was enacted in 2019, but its enforcement was delayed due to COVID-19 until June 2022. The early years focused on awareness-building, resulting in low adoption and no penalties.
- Turning Point – Enforcement: The first PDPA fine in late 2024—a penalty of THB 7 million for delayed breach notification—marked the start of real enforcement. By mid-2025, eight fines totaling over 21 million THB had been issued across multiple sectors, triggering a surge in compliance adoption.
- Key Insight: Mr. Thongjeen emphasized that "Non-compliance is an economic risk, and visible enforcement drives adoption."

2. Security Pitch and the OneFence Platform

Founded in 2020, Security Pitch evolved into a deep-tech company with over 50 employees developing "OneFence," an integrated security management platform that unites:

- Cybersecurity tools: log management, SIEM, cyber threat intelligence, vulnerability assessment.
- Privacy tools: consent and cookie management, DSAR automation, data mapping, and breach reporting modules.
- Physical security tools: AI-powered CCTV, access control, and emergency response integration.
  This convergence of cyber, physical, and privacy management enables organizations to address fragmented compliance and risk through one centralized interface.

3. Early Challenges in PDPA Adoption

Mr. Thongjeen identified seven key challenges faced during Thailand's PDPA rollout:

- Heavy education burden – Extensive training was needed before clients understood compliance value; many sought only symbolic compliance.
- Lack of regulatory templates – PDPC initially had no official Data Protection Impact Assessment (DPIA) or consent templates, forcing vendors to improvise.
- Absence of fines – No early penalties led to low urgency.
- Compliance viewed as cost – Organizations saw PDPA as an expense, not an advantage.
- Localization issues – Consent forms and UX needed cultural adaptation for Thai users.
- Siloed stakeholders – Departments operated in isolation, delaying organization-wide compliance.
- Limited executive sponsorship – Lack of top-level support slowed transformation.
  He summarized: "Compliance is 80% culture, 20% tech.".

4. Early vs. Innovation Adopters

Based on his experience, Mr. Thongjeen noted that

- Forced Adopters: Government agencies and listed companies, driven by regulatory pressure.
- Innovation Adopters: Banks, hospitals, and SOEs that used PDPA compliance as a trust or innovation KPI, e.g., a hospital branding itself as a *"PDPA-compliant medical tourism provider."* Mr. Thongjeen noted that framing compliance as innovation, not obligation, accelerated adoption and public engagement.

5. PETs as Foundations of Trust

Building on his automation work, Mr. Thongjeen highlighted Privacy-Enhancing Technologies (PETs) as central to Thailand's next phase of data protection.

- PETs such as differential privacy, homomorphic encryption, multi-party computation, zero-knowledge proofs, and trusted execution environments underpin secure AI and analytics.
- Use cases include AI-based CCTV face blurring with cryptographic audit logs, demonstrating that "PETs make privacy visible and practical."

6. Biometric Data as Economic Security

He discussed the Worldcoin case (2025), where iris scanning raised consent and data transfer concerns after 100,000 Thai users participated.

- The PDPC responded by halting operations and launching a local PET audit sandbox for biometric projects.
- Mr. Thongjeen described this as Thailand's first step toward biometric data certification, applying international standards such as ISO/IEC 24745, 27557, 27001/27701, and 23894.
- He proposed a PET certification flow requiring providers to submit designs, undergo testing by accredited labs, and earn public trust seals valid for up to two years.

7. Policy Lessons for APEC Economies

Drawing from Thailand's PDPA journey, Mr. Thongjeen offered practical policy recommendations for APEC economies:

- Regulatory agencies must lead awareness efforts and appoint authorized project champions.
- Publish PETs guidelines early, even in draft form, to guide market behavior.
- Ensure visible enforcement to create urgency and accountability.
- Frame compliance as innovation to attract voluntary participation.
- Support SMEs with modular and affordable PET adoption.
- Require PET certification for biometric and other high-risk systems.

8. Conclusion

Mr. Thongjeen concluded with a call for APEC to harmonize PET standards and certification frameworks, positioning PETs as strategic assets for digital trust and economic security.

Below is a summary of the main points from the presentation Regulatory data protection requirements in software engineering, how do we deal with interdisciplinarity?

Dr. Claudia Negri-Ribalta, University of Luxembourg, Chile, examined how the growing intersection of data protection law and software engineering demands interdisciplinary collaboration. Speaking from her dual background in law and computer science, she emphasized that regulatory data protection requirements (RDPRs) cannot be effectively implemented without bridging the communication and conceptual gaps between legal, technical, and organizational domains

1. Understanding Socio-Technical Systems and Requirements Engineering

Dr. Negri-Ribalta began by defining socio-technical information systems—not just code or machines, but an integrated network of software, business processes, infrastructure, users, and regulatory context

She introduced requirements engineering (RE) as a structured process to determine what a system should do and why. Requirements, she noted, originate from multiple stakeholders—users, organizations, legal frameworks, and even machines—and must be precise and unambiguous to be testable and enforceable

She highlighted that ambiguity is a chronic issue: when clients describe their needs in natural language, misinterpretations often occur at every level—from business analysts to developers—resulting in systems that fail to meet real-world or legal expectations.

2. Regulatory Challenges and Conceptual Misalignments

Dr. Negri-Ribalta identified five systemic issues that complicate compliance with RDPRs:

- Different conceptualizations between lawyers and engineers—legal norms depend on context ("it depends"), while software engineering requires unambiguous specifications.
- Ambiguity in legal drafting—terms like "quality," "accessibility," or "fairness" lack technical definitions, creating uncertainty in software design. For example, Chile's proposed digital platform law required "universally accessible, quality, and non-discriminatory services" without defining measurable criteria
- Conflicting jurisdictional demands—regulations across markets may contradict, such as requirements for encryption backdoors versus mandates for strong encryption.
- Technical infeasibility—certain regulatory demands cannot be implemented without compromising system integrity.
- Misconceptions in practice—many engineers conflate data protection with cybersecurity, focusing only on confidentiality or access control, while ignoring principles like data minimization or rectification

She cited research showing that while 90% of software developers understand encryption, fewer than 40% are familiar with privacy principles such as rectification or data expiry.

3. Bridging the Gap: Methods and Tools

Dr. Negri-Ribalta proposed a set of practical approaches to improve interdisciplinary collaboration:

- Establish common ground through taxonomies and ontologies to unify language across disciplines.
- Build interdisciplinary teams combining lawyers, engineers, business analysts, and ethicists to co-design systems and policies.
- Identify conflicting requirements early in development to reduce costly rework.
- Use diagrams instead of prose to minimize misinterpretation—models such as BPMN (Business Process Modeling Notation) and Socio-Technical Security and Privacy Modeling Languages (STS-ml) translate legal norms into visual workflows understandable to all stakeholders

She highlighted the LINDDUN framework, a privacy threat analysis method, as a proven tool to identify privacy risks and document mitigation strategies across system design stages.

4. Persistent and Emerging Challenges

Despite methodological progress, Dr. Negri-Ribalta noted several persistent barriers:

- Communication gaps between disciplines remain the greatest obstacle.
- Evolving regulations demand adaptive systems that can evolve without full redesign.
- Metrics and testing for compliance are still immature—there is no universal benchmark to measure “GDPR compliance.”
- Implicit understanding—trust and shared intuition between professionals—takes years to build but is essential for effective collaboration

5. Recommendations and Conclusion

Dr. Negri-Ribalta concluded with a call to action:

- Continue developing new interdisciplinary tools and methods in both academia and industry.
- Maintain spaces for dialogue between legal, technical, and policy communities.
- Involve lawyers early in software development, particularly during the requirements phase.
- Promote the role of “public-interest technologists” who combine technical literacy with policy awareness.

- Above all, foster empathy and understanding—the human element essential to bridging law and technology

She closed by reminding participants that building trustworthy digital systems is not purely a technical or legal task, but a collective human endeavor grounded in communication, cooperation, and shared responsibility.

Key Takeaways from Plenary II Panel Discussion

In this session featuring Mr. Pakorn Thongjeen (Thailand) and Dr. Claudia Negri-Ribalta (Chile), moderated by Dr. Hsiao (Chinese Taipei), the discussion examined how regulatory frameworks, technical practices, and cross-disciplinary collaboration can collectively advance privacy protection. The dialogue explored the practical implications of Thailand's PDPA, the role of AI and large language models in compliance, and the cultural dimensions of regulatory design.

1. Understanding Thailand's PDPA: Anonymization vs. Pseudonymization

Mr. Thongjeen explained that under Thailand's Personal Data Protection Act (PDPA), anonymized data is not considered personal data. However, if anonymized information can be combined with other data to re-identify individuals, it "may in some way" still fall under the PDPA. This interpretation highlights Thailand's pragmatic recognition that identifiability depends on context and available data sources.

2. The Role of AI and LLMs in Compliance

Dr. Negri-Ribalta noted that AI in compliance extends far beyond generative AI. Since the 1980s, experts have developed AI-based expert systems to help verify whether software systems and privacy policies meet regulatory requirements.

- Emerging Applications: Recent work at Carnegie Mellon University and the University of Luxembourg explores using large language models (LLMs) to automatically evaluate the consistency and validity of privacy policies.
- Model-Driven Engineering: Research from the Polytechnical University of Valencia demonstrates how AI can generate or validate compliance-ready code.
- Limitations: She emphasized that these tools are still in the proof-of-concept stage and not widely adopted. Ethical and adaptability challenges remain—particularly how AI systems can adjust when laws change.

3. Breaking Silos and Building Interdisciplinary Capacity

Both speakers emphasized that communication and education are critical for advancing data protection.

- Mr. Thongjeen’s Approach: Drawing on Thailand’s PDPA rollout, he suggested three practical strategies for privacy transformation:
  - (1) Show empathy and communicate positively—acknowledge that adapting to new laws can be difficult, and motivate others as *first movers*.
  - (2) Establish a shared language that bridges technical, legal, and organizational perspectives.
  - (3) Maintain optimism and patience throughout implementation.
- Dr. Negri-Ribalta’s View: She called education the “silver bullet.” Computer scientists should learn basic legal frameworks, while lawyers should become comfortable with programming and data analysis. Continuous internal training helps companies build interdisciplinary experts and integrate privacy across domains.

4. Localized Regulation and Policy Lessons for APEC Economies

When asked about policy localization and regional comparison, Mr. Pakorn described personal data protection as the *foundation of the digital economy* that builds trust and resilience.

- Recommendations for Economies like Chinese Taipei:
  - (1) Publish localized guidelines or templates early, even in draft form, to allow public review and improvement.
  - (2) Provide incentives for local innovation: Thailand’s PDPC offers tax reductions of up to 2,000% for companies using “Made in Thailand” certified cybersecurity products.
- Localization and Cultural Fit: He emphasized that localization is crucial for practical compliance, referencing the Worldcoin iris-scanning case in Thailand—although the company followed GDPR standards, many local users did not understand the consent forms, underscoring the need for culturally adapted implementation.
  Dr. Negri-Ribalta added that while APEC and OECD privacy frameworks offer alignment, a single global law may not be realistic. She observed that cultural norms—such as collective consent in some African and Latin American societies—differ from the individual-centric consent model in Asia-Pacific. Thus, while the *method* of obtaining consent can be standardized, the *concept* should remain culturally adaptable.

5. Biometric Data Governance under the PDPA

On biometric data collection, Mr. Thongjeen explained that explicit, freely given consent is required under Thailand’s PDPA.

- Corporate Use: When companies act as data controllers (e.g., using facial recognition for building access), they must provide clear privacy notices detailing purpose, storage, and security measures.
- Law Enforcement Use: Police are data controllers when collecting biometric data during investigations. Subjects can request deletion, but the police may legally reject such requests. He stressed that transparency and notification are essential for maintaining trust in biometric data management.

6. Integrating Privacy into Agile Development

Both speakers discussed balancing development speed with privacy compliance.

- Privacy Champion Concept: Mr. Thongjeen introduced the idea of a Privacy Champion—a senior leader empowered to ensure privacy is embedded in all stages of software development. In his company, all new employees receive PDPA training to reinforce this culture.
- Adapting to Agile Practices: Dr. Negri-Ribalta recommended integrating privacy into agile frameworks such as Scrum. Each iteration can include a trained Privacy Champion who documents privacy requirements.
- Cultural Dimension: She emphasized fostering a culture of privacy awareness rather than expecting perfect “privacy by design.”
- Real-World Example: In a blockchain project, her team met monthly with the Data Protection Officer for two hours and appointed a privacy ambassador to ensure consistent compliance throughout design and development.

2.4 Plenary III: Practical Application

Below is a summary of the main points from the presentation *Differential Privacy: Case Study*:

Dr. Chia-Mu Yu, Associate Professor at National Yang Ming Chiao Tung University, Chinese Taipei, delivered a presentation focusing on Differential Privacy (DP) use cases, exploring both theoretical foundations and practical deployment challenges.

1. Overview of PETs

Privacy-Enhancing Technologies (PETs) are defined as methods and tools that help protect individual privacy and data security. Examples include Homomorphic Encryption (HE), Zero-Knowledge Proofs (ZKP), Differential Privacy (DP), Federated Learning (FL), Secure Multi-Party Computation (SMPC), and anonymization.

PETs are not a panacea; they address two often contradicting requirements: privacy and data utility. Users must select a particular PET based on the application scenario. Key questions include whether the application involves data release or collection, the need for an exact result versus statistical value, available computing resources, and whether record linkage is necessary.

2. Differential Privacy (DP) Theory and Mechanics

Differential Privacy (DP) is highlighted as a popular PET. The theoretical foundation rests on a simple concept: if two databases differ by only one person's record, any output from a query should be statistically the same for both databases.

DP is achieved primarily through the injection of noise into the data or the query results. The core challenge for DP systems and algorithms is finding the right balance: sufficiently large noise guarantees high privacy, but the data becomes unusable; very small noise maintains utility but fails to protect privacy.

3. Types of Differential Privacy

DP can be categorized based on the interaction model:

- Interactive DP: This approach involves constantly querying a database and receiving results that have been injected with noise. This is primarily used to prevent insider threats.
- Non-Interactive DP: This involves processing a dataset once using DP, and then releasing the processed data to the public. The current paradigm often uses DP Synthetic Data.
- Local DP (LDP): This is used for data collection. The user contributes data that has been randomly distorted. Although individual data is noisy, the entity collecting a large volume can mathematically derive

the overall distribution.

4. Real-World Deployment Use Cases

LinkedIn’s Labor Market Insights (Data Release)

During COVID-19, LinkedIn needed to release statistics to provide timely market demand insights. LinkedIn focused on event-level privacy, protecting whether an individual or company participated in a specific hiring event. They selected the top 1,000 employers, added DP noise to the hiring counts, and published the top 20 companies based on the noisy counts.

Israel’s National Registry of Live Births (Dataset Release)

The Israeli government aimed to release its local birth registry data for public health and policy research. They utilized DP Synthetic Data to release a modified dataset, aiming for Formal Privacy and Face Privacy. They faced challenges regarding user expectation; medical units found purely synthetic records "too fake," so they added a faithfulness requirement.

Collaboration with City Government (Record Linkage)

This involved linking three separate government datasets related to traffic accident victims to evaluate process efficiency, but regulatory constraints prohibited data sharing. Since the primary need was statistical calculation, they applied Local DP (LDP) separately to the records. A design choice was necessary regarding missing values.

5. Observations and Lessons Learned

Dr. Chia-Mu Yu shared his views on four main lessons derived from these deployments:

- Statistics over ML: In most real-world applications, simple statistics are sufficient.
- Record Linkage: Current DP deployments rarely consider the need for record linkage across multiple datasets.
- Hybrid Approach: A hybrid approach is often required in real-world applications.
- Face Privacy: "Face privacy" often requires extra processing that is not strictly necessary for formal privacy guarantees but is needed to satisfy the public's psychological need.

6. Conclusion

Dr. Chia-Mu Yu noted that DP has evolved from a purely academic concept to one with growing real-world demand and practical deployment. However, unlike simple encryption, DP implementation requires careful consideration regarding the choice and magnitude of the noise to ensure both security and utility.

Below is a summary of the main points from the presentation *The Government's Critical Role for Responsible Development of Privacy-Enhancing Technologies*:

Ms. Jun Chu, Head of Cybersecurity and Privacy Policy for Asia Pacific at Google in Singapore, provided an overview of Google's approach to Privacy-Enhancing Technologies (PETs) and detailed five core policy recommendations for governments to encourage their widespread adoption.

1. Google’s Approach to PETs

Google views PETs as crucial tools that enable the use of data to improve products without compromising anyone's privacy and security. The company has been a long-time advocate of PETs, adopting what it terms "privacy by innovation."

The rise of Generative AI (Gen AI) is accelerating the use of PETs. Since data is "king" in the age of AI, and greater data access improves AI models, there is a necessary tradeoff between utility and data protection. PETs are considered a key method to increase the utility of AI without sacrificing security or privacy.

PETs generally fall into two broad categories: isolation protection (keeping data isolated, using techniques like Trusted Execution Environments or Federated Learning) and data anonymization (using techniques like Differential Privacy).

Google has invested significantly in PETs for over a decade, pioneering techniques like federated learning and making major progress in differential privacy.

2. Real-World Use Cases at Google

Ms. Chu provided several examples of PETs in action within Google’s products:

- Google Maps Popular Times: This feature uses differential privacy and aggregation to show how busy a place is without tracking exact individual movements.
- Google Trends: This provides insights into popular search interests without compromising user privacy through anonymization, categorization, and aggregation.
- Other Uses: Google also uses TEEs for confidential matching in advertising and applies differential private synthetic data to train models for detecting unsafe content.

3. Challenges to PETs Adoption

The adoption of PETs is still "relatively nascent" and unevenly distributed across the private and public sectors and different economies. The challenges are categorized broadly as: organizational, resource allocation, lack of technical expertise, considerable cost of implementation, and, critically, a lack of regulatory clarity and certainty.

4. Policy Recommendations for Governments

Ms. Chu emphasized that governments have a particularly critical role to play in accelerating PETs adoption. She outlined five core recommendations:

- Champion Use and Lead by Example: Governments should use PETs in their own systems and incentivize their use in government procurements. They should also publish domestic strategies, fund PETs requests, and host workshops.
- Invest in Research and Upskilling: Governments can lower barriers by increasing access to resources like open-source tools. They should invest in education and training and fund high-risk, high-reward foundational research.
- Promote Openness and Collaboration: Governments should work to better align data protection and sharing rules across economies. Specific actions include requiring government-funded research to be made public when appropriate and supporting open-source contributions.
- Encourage Development of Technical Standards and Implementation Guidelines: Standards are key to reducing regulatory uncertainty. Governments should actively work with international standards bodies to align policies and best practices.
- Smart Policies & Regulatory Incentives (Risk-Based Framework): This involves implementing policies that motivate "privacy by innovation." Key components include enabling experimentation through regulatory sandboxes, taking a tiered approach to data identifiability, providing legal recognition for PETs, and considering PETs in enforcement.

Ms. Chu concluded by emphasizing that PETs are building blocks for innovation, and a coordinated "whole-of-government approach" is essential for creating a cohesive strategy across ministries and departments.

Key Takeaways from Plenary III Panel Discussion

In this panel discussion featuring speakers from Singapore; Chinese Taipei; and the United States, participants explored the practical, technical, and policy challenges in advancing the adoption of Privacy-Enhancing Technologies (PETs). The dialogue highlighted the role of regulatory sandboxes, the importance of technical literacy, and the balance between innovation and governance in privacy-preserving solutions.

1. Singapore’s Regulatory Sandbox for PETs

- Collaborative Framework: Ms. Chu explained that Singapore’s PET Sandbox is a multi-year initiative by the IMDA, involving private companies from healthcare, finance, and advertising sectors.
- Role of Partners: IMDA acts as regulator and funder, providing policy guidance and financial support, while large technology firms—such as Google—offer technical expertise to local start-ups.
- Outcomes and Oversight: Participants conduct applied research and share periodic progress reports on implementation challenges. Findings are presented annually during Singapore’s *Personal Data Protection Week PET Summit*, ensuring transparency and continuous learning across sectors.

2. Government Access and Legal Boundaries

When asked about government access to user data, Ms. Chu emphasized that this issue is distinct from PETs and falls strictly within legal processes. Data requests for law enforcement or local security system must follow established legal procedures. Google evaluates each request under its internal policy to ensure compliance with law while safeguarding user privacy. She clarified that such questions are fundamentally legal, not policy-based, and should be addressed by legal professionals.

3. Technical Challenges in PET Implementation

Dr. Yu noted that while working with governments posed few procedural difficulties, the real challenge lies in understanding the complexity of PETs themselves.

- PETs like Differential Privacy (DP) or Homomorphic Encryption (HE) are not plug-and-play tools; their parameters must be correctly configured to ensure both privacy and utility.
- A misconfigured PET, or the wrong choice of method for a given scenario, can completely undermine protection.

  He stressed the importance of selecting appropriate PETs for each use case and providing technical education to ensure correct deployment.

4. Misconceptions and the Need for Education

Both speakers identified widespread misunderstandings about PETs:

- From Dr. Yu’s Experience: In financial collaborations using *DP synthetic data*, clients often misunderstood its nature. Some assumed that if the data “looked too similar” to the real dataset, it was unsafe, while others treated synthetic data as real, performing operations like SQL joins between unrelated datasets. Such misconceptions highlight the urgent need for education and training on what PETs can and cannot achieve.

- From Ms. Chu's Policy Perspective: Many policymakers and companies view PETs as a *"silver bullet"* that can preserve privacy and utility simultaneously in all contexts. She underscored that PETs inherently involve trade-offs—too much noise can destroy utility, and no single PET can solve every privacy challenge. Hence, a combination of complementary PETs and public funding for high-risk, high-reward research is essential to drive responsible innovation.

5. PETs in the Age of Quantum and Emerging AI

- Quantum Computing: Dr. Yu explained that PETs relying on anonymization—like DP—will likely remain secure even in the quantum era, as they remove information entirely rather than hiding it. However, cryptographic PETs such as HE could be affected, though this remains uncertain. He also cautioned that some PETs, such as Federated Learning, may already face vulnerabilities from conventional computing attacks.
- Generative AI and LLMs: Ms. Chu discussed Google's recent guidance on privacy in generative AI, emphasizing two policy priorities:
  (1) Protect the availability of public data, since PETs enable access to valuable datasets essential for improving AI model performance.

  (2) Focus on output integrity rather than input deletion, as machine unlearning—the ability to remove specific data from AI models—is still technically infeasible and extremely resource-intensive. PETs can instead help reduce downstream risks like hallucination or prompt injection.

3. Integrated Overall Summary

The workshop focused on how PETs can be governed, engineered, and applied in practice. Speakers agreed that a principles-based, technology-neutral approach, paired with practical instruments and cross-disciplinary work, is key to turning PETs into sustainable practice across sectors and economies.

I. Regulation & Policy

Core themes

- Keep laws principles-based and technology-neutral, supported by guidance, interpretation policies, and regulatory sandboxes to improve predictability.
- Clarify the status and scope of anonymization to reduce uncertainty and support adoption; use proportionate recognition or certification where suitable.
- Maintain cross-border trust through continued APEC-level dialogue and alignment with related fora, while preserving domestic compliance.
- Localize templates and notices in clear, plain language to fit local context and public understanding.

Recommendations

- Use guidance, interpretation policies, and sandboxes to set clear supervisory expectations and lower adoption risk.
- Restate definitions and boundaries for anonymization and related compliance duties.
- Continue regional coordination on terminology and expectations in support of trusted cross-border data flows.
- Publish draft templates early, invite feedback, and adapt materials for local use.

II. Technology & Engineering

Core themes

- Select PETs to fit the use case and configure them correctly; validate outcomes against stated privacy and utility goals.
- Combine methods when needed and manage trade-offs in performance, scalability, and governance cost.
- Translate legal requirements into engineering-ready specifications using shared vocabularies and visual models to ensure implementability and auditability.
- Track emerging risks and developments with a cautious, rolling assessment.

Recommendations

- Support configuration and verification with standardized checklists and testing notes.
- Run small, time-boxed pilots in regulatory sandboxes and produce reusable artifacts such as risk assessments and process templates.
- Align terminology and modeling conventions across teams to reduce ambiguity in design and review.

III. Practical Implementation

Core themes

- Embed privacy into development. Designate a Privacy Champion with sufficient authority, and keep regular alignment with compliance functions.
- Build capability across policy, legal, and technical roles through sustained training and clear internal procedures.
- Capture and share what works. Plain-language communication and accessible materials help build trust and day-to-day usability.

Recommendations

- Set a steady cadence for cross-disciplinary coordination and peer exchange across agencies, sectors, and teams.
- Publish reusable documents—process flows, forms, and checklists—to speed replication.
- Provide clear communication materials in plain language to support local rollout and public understanding.