

# 13th Asia Privacy Bridge Forum 2024

## International Collaborations in Trustworthy AI Governance and Privacy

Day  
1

**Oct 17 (Thursday) 10:00~13:40**

#733, 7th Floor, Chang Ki Won International Conference Hall,  
Yonsei-Samsung Library, Yonsei University

Day  
2

**Oct 18 (Friday) 10:00~16:20**

#B126 Grand Ballroom, The Commons,  
Yonsei University



# Welcoming Remarks

Distinguished guests, ladies and gentlemen,

It is my great pleasure to welcome you to the 13th Asia Privacy Bridge Forum and Privacy Global Edge event. On behalf of Yonsei University, I am truly honored to be part of this significant occasion. I extend a warm welcome to Chairman, Hak-soo Ko of the Personal Information Protection Commission in the Republic of Korea and Executive Director, Ivin Ronald D.M. Alzona of the National Privacy Commission in the Republic of Philippines. Your presence underscores the importance of our gathering today.

As we embark on this journey into the age of AI, we face both exciting opportunities and critical challenges. To address these challenges, I believe that developing trustworthy AI and establishing effective global AI governance are crucial. The 13th Asia Privacy Bridge Forum and Privacy Global Edge focused on 'International Collaborations in Trustworthy AI Governance and Privacy,' which is a timely and significantly important topic.

The Barun ICT Research Center and the Korea CPO Forum have been at the forefront of addressing the growing threat of personal data protection breaches. As evidenced by the recent viral deepfake video of a South Korean political figure, these deceptive AI-generated videos pose a serious risk to democratic processes. This incident underscores the urgent need for global collaborations. To combat this and safeguard individual privacy, collaborative efforts among regulatory bodies, experts, and practitioners are essential.

Above all, the forum has attracted a diverse range of stakeholders, demonstrating its global influence in shaping the future of data privacy and protection. We have attracted participants from 19 countries, including China, Japan, Taiwan, Singapore, Indonesia, Malaysia, and India. The involvement of international organizations like the OECD and APEC, leading NGOs, 15 major government agencies including personal information protection commissions, 20 key institutions and research institutes focused on personal information protection from each nation, 7 leading global law firms like Baker McKenzie, a diverse range of global big tech companies such as Meta, MS, Google, eBay, NVIDIA, Facebook, ASML, NAVER, Kakao, NEXON, and NC Soft, and around 40 major universities worldwide including Singapore Management University have taken part in this event.

One of the key achievements of this forum is its focus



on examining AI technology and privacy issues from an Asian perspective on AI and privacy. Asia's rich cultural and historical diversity provides a valuable lens for examining these complex issues. By fostering collaboration and sharing insights across the region, I firmly believe this forum provides a significant opportunity to amplify Asia's voice in the trustworthy AI governance conversations and seek international collaborations.

Esteemed participants, we are living in one of the most exciting and challenging periods in human history. AI technology offers us limitless possibilities, but it also demands our wise choices and collaboration. I sincerely hope that this Asia Privacy Bridge Forum and Privacy Global Edge will serve as a milestone in addressing the challenges of the AI era and creating a more just, equitable, and prosperous future. We look forward to your enthusiastic participation and insightful discussions.

In conclusion, I would like to express my heartfelt thanks to Chairman Tae-myung Chung of the Korea CPO Forum and Executive Director Beomsoo Kim of the Barun ICT Research Center at Yonsei University for organizing this meaningful event. I also extend my gratitude to all the faculty members and staff of both institutions who have dedicated their efforts to prepare for this forum. May you all gain valuable insights and have a memorable time at the 13th Asia Privacy Bridge Forum and Privacy Global Edge event.

Thank you.

**Won-Yong LEE**

Senior Vice President for Research Affairs,  
Yonsei University



---

# Invitation to 2024 Asia Privacy Bridge Forum

Recent advancements in AI technology have accentuated the growing importance of data governance and privacy, while also highlighting the need for international cooperation.

The 13th Asia Privacy Bridge Forum, in conjunction with Privacy Global Edge, will convene under the theme "International Collaborations in Trustworthy AI Governance and Privacy." This forum offers a unique opportunity for learning and growth in your respective fields. It aims to engage in profound discussions on global collaborative strategies to build a happier society in the AI era. The myriad of ethical issues surrounding data protection and privacy, particularly when intertwined with artificial intelligence technologies, necessitate proactive cooperation among nations to strike an equilibrium between technological progress and regulation, thus fostering corporate innovation.



Consequently, the 13th Asia Privacy Bridge Forum will go beyond the mere exchange of knowledge pertaining to personal information protection. It will serve as a platform for a thorough analysis of the changes and impacts that artificial intelligence technology will have on various aspects of our lives, including work, education, entertainment, and politics. Furthermore, it will provide an opportunity to collectively generate innovative ideas and collaborative measures across these domains.

We are confident that your active participation will make a substantial contribution to establishing a forum for discussions that will shape a better future through the 13th Asia Privacy Bridge Forum.

**Beomsoo KIM**  
Director, Barun ICT Research Center

# Program

**Day1** Thursday, October 17th

10:00AM~13:40PM

#733, 7th Floor, Chang Ki Won International Conference Hall, Yonsei-Samsung Library, Yonsei University

**09:30-10:00**

Registration / Coffee Break

**10:00-10:40**

**Plenary Session 1 : Navigation Gen AI and Trustworthy AI Governance for the Future**

- Chair : Baekcheol Jang

Professor, Graduate School of Information, Yonsei University

**"Singapore's Evolving Approach to AI Governance"**

- Jason Grant ALLEN

Associate Professor, Singapore Management University,  
Yong Pung How School of Law, Singapore (Pre recorded Presentation)

**"Data Protection, Competition, and AI Governance : The Importance of Data Portability and ADM Governance in Data Protection Laws"**

- Qing HE

Assistant Professor, Beijing University of Posts and Telecommunication, China

**"Designing Accountable Community in the Emerging AI Period"**

- Kohei Kurihara

CEO, Privacy by Design Lab, Japan

**10:50-11:30**

**Plenary Session 2 : Reconciling Data Protection and Competition Laws in the Age of AI**

- Chair : Ha Young Kim

Professor, Graduate School of Information, Yonsei University

**"Taking Stock : Data Protection, Privacy and Competition Law"**

- Orla Lynskey

Professor, University College London, Law School, UK  
(Pre recorded Presentation)

**"Reproduction of Personas with AI and the Right of Publicity"**

- Kunifumi SAITO

Associate Professor, Faculty of Policy Management, Keio University, Japan

**"Personal Data & Generative AI"**

-Dae-Hee Lee

Professor, Korea University, Law School, Korea

---

**11:30-13:00**

Lunch

---

**13:00-13:40**

**Plenary Session 3 : Digital Shield : Safeguarding Privacy and Data for Vulnerable Users**

- Chair : **Hyojin Jo**

Professor, Graduate School of Information, Yonsei University

---

**“Challenges for Non-Digital Natives to Protect the Rights of Digital Natives”**

- **Byungsoo Jung**

Director, Children’s Rights Division,  
The Korean Committee for UNICEF, Republic of Korea

---

**“Children and AI: Key Issues to Consider to Empower and Protect Them”**

- **Steven Edwin Vosloo**

Policy Specialist, Digital Engagement and Protection, UNICEF Innocenti, Italy  
(Pre recorded Presentation)

---

**“Safeguarding and Empowering Vulnerable Children in the Digital Age :  
Save the Children’s Global Initiatives”**

- **Jeffrey DeMarco**

Senior Advisor, Protecting Children from Digital Harm,  
Save the Children’s global Safe Digital Childhood Initiative, UK

---

**13:50-14:20**

**Signing ceremony of a Joint Declaration**

The 13th Asia Privacy Bridge Forum will convene representatives from ten countries, including Philippines, to issue a joint declaration underscoring the critical importance of privacy and international cooperation in the evolving landscape of AI technology.

---

**15:00-16:30**

**Side Event at Bae, Kim & Lee LLC (법무법인 태평양) (Invitation only)**

- **Jae-Suk Yun** CPO, ASML KOREA
- **Susan Park** Senior Foreign Attorney, Bae, Kim & Lee LLC
- **Taeuk Kang** Partent, Bae, Kim & Lee LLC
- **Sanghoon Shin** Senior Foreign Attorney, Bae, Kim & Lee LLC
- **Sangmi Chai** Professor, Ewha Women’s University

# Program

Day2 Thursday, October 18th

10:00AM~16:20PM

#B126 Grand Ballroom, The Commons, Yonsei University

---

**09:30-10:00** Registration / Coffee Break

---

**10:00-10:40**

Keynote

**"Privacy Protection and Harness in the Age of Gen AI"**

- **Seong-yeob LEE**

Chair, Korea Data Law and Policy Society

---

**10:40-11:20**

Keynote

**"Navigating the Future : AI Governance and Data Privacy in the Philippines  
— A Regulatory Perspective"**

- **Ivin Ronald D.M. Alzona**

Executive Director, National Privacy Commission, Republic of the Philippines

---

**11:20-12:00**

Opening / Welcoming Remarks

---

**12:00-13:20**

Lunch

---

**13:20-14:00**

**Plenary Session 4 : Platform Governance and AI Accountability**

- **Chair : Jongsoo YOON**

Attorney, Lee & Ko

---

**"META's Approach to Responsible AI"**

- **Da-young YOO, on behalf of Raina Yeung**

Director of Privacy and Data Policy, Engagement, APAC at Meta, Singapore

---

**"Responsible AI in Malaysia: The Role of Data Protection Policy"**

- **Jillian Chia**

Attorney, SKRINE, Malaysia

---

**"Regulatory Landscape for Generative AI in Japan: Insights and Outlook"**

- **Hitomi Iwase**

Attorney, Nishimura & Asahi, Japan



---

**14:00-14:40**

**Plenary Session 5 : What is Data Sovereignty? Global Cross-Border Privacy Rules (GCBPRs) and Cooperation in Investigation and Enforcement**

- Chair : Kwang Bae PARK  
Attorney, Lee & Ko

---

**“South Korea’s Regulatory Framework for Cross-Border Data Transfer Policies”**

- Jeongsoo LEE  
Deputy Director, Personal Information Protection Commission, Republic of Korea

---

**“Data Sovereignty in Vietnam: Legal Requirements, Enforcement Trends, and Global CBPRs Interactions”**

- Huyen-Minh Nguyen  
Senior Associate, BMVN International LLC, Vietnam

---

**“Global Cross-Border Transfers:  
A Comparative Analysis of China, Hong Kong, and Beyond”**

- Dominic Edmondson  
Special Counsel, Baker McKenzie, Hong Kong

---

**14:40-15:00**

Coffee Break

---

**15:00-15:40**

**Plenary Session 6 : Fair Use of Data**

- Chair : Byungnam LEE  
Senior Advisor, Kim & Chang

---

**“Exploring Utility and Privacy in Synthetic Data”**

- Joseph Hyun-Tae Kim  
Associate Professor, Yonsei University,  
Department of Applied Statistics, Republic of Korea

---

**“Guidelines for Using Pseudonymization for Unstructured Data in South Korea”**

- Hyun Joon Kwon  
Former Director, Personal Data Secure Usage Division,  
Korea Internet & Security Agency, Republic of Korea

---

**15:40-16:20**

Closing Ceremony

# Table of Contents



## Oct 17 (Thursday) 10:00~13:40

#733, 7th Floor, Chang Ki Won International Conference Hall,  
Yonsei-Samsung Library, Yonsei University

### Session 1. Navigation Gen AI and Trustworthy AI Governance for the Future

Chair: Beakcheol Jang (Professor, Graduate School of Information, Yonsei University, Republic of Korea)

1. Jason Grant ALLEN (Associate Professor, Singapore Management University, Yong Pung How School of Law, Singapore)  
Singapore's Evolving Approach to AI Governance ..... 15
2. Qing HE (Assistant Professor, Beijing University of Posts and Telecommunications, China)  
Data Protection, Competition, and AI Governance: The Importance of Data Portability and ADM Governance  
in Data Protection Laws ..... 23
3. Kohei Kurihara (CEO, Privacy by Design Lab, Japan)  
Designing Accountable Community in the Emerging AI period ..... 37

### Session 2. Reconciling Data Protection and Competition Laws in the Age of AI

Chair: Ha Young Kim (Professor, Graduate School of Information, Yonsei University, Republic of Korea)

1. Orla Lynskey (Professor, University College London, Law School, UK)  
Taking Stock: Data Protection, Privacy, and Competition Law ..... 51
2. Kunifumi SAITO (Associate Professor, Faculty of Policy Management, Keio University, Japan)  
Reproduction of Personas with AI and the Right of Publicity ..... 59
3. Dae-Hee Lee (Professor, Korea University, Law School, Republic of Korea)  
Personal Data & Generative AI ..... 69

### Session 3. Digital Shield: Safeguarding Privacy and Data for Vulnerable Users

Chair: Hyojin Jo (Professor, Graduate School of Information, Yonsei University, Republic of Korea)

1. Byungsoo Jung (Director, Children's Rights Division, The Korean Committee for UNICEF, Republic of Korea)  
Challenges for non-digital natives to protect the rights of digital natives ..... 85
2. Steven Edwin Vosloo (Policy Specialist, Digital Engagement and Protection, UNICEF Innocenti, Italy)  
Challenges for Non-digital Natives to Protect the Rights of Digital Natives ..... 93
3. Jeffrey DeMarco (Senior Advisor, Protecting Children from Digital Harm, Save the Children's Global Safe Digital Childhood  
Initiative, UK)  
Safeguarding and Empowering Vulnerable Children in the Digital Age: Save the Children's Global Initiatives ..... 101

**Oct 18 (Friday) 10:00~16:20**

#B126 Grand Ballroom, The Commons,  
Yonsei University

### Keynote Speech

Ivin Ronald D.M. Alzona (Executive Director, National Privacy Commission, Republic of the Philippines)

Navigating the Future: AI Governance and Data Privacy in the Philippines – A Regulatory Perspective ..... 111

### Session 4. Platform Governance and AI Accountability

Chair: Jongsoo YOON (Attorney, Lee & Ko, Republic of Korea)

1. Raina Yeung (Director of Privacy and Data Policy, Engagement, APAC at Meta, Singapore)  
Meta's Approach to Responsible AI ..... 123
2. Jillian Chia (Attorney, SKRINE, Malaysia)  
Responsible AI in Malaysia: The Role of Data Protection Policy ..... 125
3. Hitomi Iwase (Attorney, Nishimura & Asahi, Japan)  
Regulatory Landscape for Generative AI in Japan: Insights and Outlook ..... 133

### Session 5. What is Data Sovereignty? Global Cross-border Privacy Rules (GCBPRs) and Cooperation in Investigation and Enforcement

Chair: Kwang Bae PARK (Attorney, Lee & Ko, Republic of Korea)

1. Jeongsoo LEE (Deputy Director, Personal Information Protection Commission, Republic of Korea)  
South Korea's Regulatory Framework for Cross-Border Data Transfer Policies ..... 143
2. Huyen-Minh Nguyen (Senior Associate, BMVN International LLC, Vietnam)  
Data Sovereignty in Vietnam: Legal Requirements, Enforcement Trends, and Global CBPRs Interactions ..... 149
3. Dominic Edmondson (Special Counsel, Baker McKenzie, Hong Kong)  
Global Cross-Border Transfers: A Comparative Analysis of China, Hong Kong, and Beyond ..... 157

### Session 6. Fair Use of Data

Chair: Byungnam LEE (Senior Advisor, Kim & Chang, Republic of Korea)

1. Joseph Hyun-Tae Kim (Associate Professor, Yonsei University, Department of Applied Statistics, Republic of Korea)  
Exploring Utility and Privacy in Synthetic Data ..... 175
2. Hyun Joon Kwon (Former Director, Personal Data Secure Usage Division, Korea Internet & Security Agency, Republic of Korea)  
Guidelines for Using Pseudonymization for Unstructured Data in South Korea ..... 177



Day  
**1**

# Session 1

## Navigation Gen AI and Trustworthy AI Governance for the Future

### Chair

Beakcheol Jang

Professor, Graduate School of Information,  
Yonsei University, Republic of Korea



### 1

Jason Grant ALLEN

Associate Professor, Singapore Management  
University, Yong Pung How School of Law, Singapore



### 2

Qing HE

Assistant Professor, Beijing University of Posts  
and Telecommunications, China



### 3

Kohei Kurihara

CEO, Privacy by Design Lab, Japan







## Singapore's Evolving Approach to AI Governance



Jason Grant ALLEN

Associate Professor, Singapore Management University,  
Yong Pung How School of Law, Singapore



### BIOGRAPHY



Jason Grant Allen is an Associate Professor of Law and Director of CAIDG, an interdisciplinary research center focused on the law and regulation of emerging digital technologies at SMU Yong Pung How School of Law. He is also an Adjunct Associate Professor (an honorary appointment) at his alma mater, the University of Tasmania School of Law, a Research Affiliate at the Cambridge Centre for Alternative Finance at the Cambridge Judge Business School, and an Urban Fellow at the SMU College of Integrative Studies Urban Institute.

He graduated from law school during the GFC (and, he would later discover, the birth of crypto). Right after graduation, he packed off to New York, cramming for the Bar Exam in 2008, and watched modern history unfold on Wall Street. This led him to pursue a postgraduate degree in international economic law and sparked a lifelong fascination with the changing world we live in.

He enjoys working where law meets emerging technologies. For the past few years, he has been busy with blockchain and DLT. He is interested in money (whatever that may be today!), decision systems, and the interfaces between the "real world" and "virtual" spaces of social and economic interaction—in short, wherever law, in all its path-dependent glory, meets with technology-driven (but all-too-human) behaviors.





# Singapore's Evolving AI Governance Framework

Jason Grant ALLEN  
Associate Professor of Law, SMU Yong Pung How School of Law

## Introduction



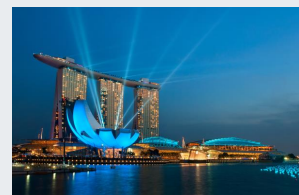
**Opening Remarks:** Introduction to AI governance as a key area of policy and regulation in Singapore.



**Relevance:** Singapore is recognized as one of the most AI-ready jurisdictions globally, with AI as a strategic technology for economic development.



**Goals of the Presentation:** To provide an overview of Singapore's AI governance framework, key policies, and international influence.



## Context & Key Characteristics of Singapore’s AI Governance Approach



**Smart Nation Initiative:** Alignment with Singapore’s digital transformation vision.



**Collaborative Governance:**

- **Consensus Building:** Involvement of government, industry, and citizens.
- **Voluntary or Quasi-Regulation:** Emphasis on standards, audit frameworks, and soft law instruments (e.g., AI Verify).



**Responsible Optimism:** Balancing innovation with public trust and safety.

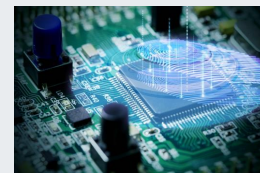


**Risk-and-Principles Approach:** Comprehensive but not complete coverage of GenAI data, model, content generation, and ethics—Cf rules-based (China) and risk-based (EU) approach

## Singapore’s AI Governance Milestones

▪ **Early Mover Status:**

- **Model Framework for AI Governance:** Released in 2019 and updated in 2020.
- **First AI Governance Testing Framework:** AI Verify, launched in 2022.



▪ **NAIS 1.0 and 2.0:**

- **National AI Strategy:** Holistic digital transformation through AI. NAIS 2.0. more focussed on public good (beyond that assumed within economic development), global competition (and competitiveness), and on building a more robust AI ecosystem rather than national projects.
- **New Systems and Enablers:** Focusing on government-industry-research collaboration, AI talent development, and trusted infrastructure.
- **(State’s Dual Role as Regulator and Investor/Purchaser:** Mirrored in other Asian Jurisdictions (and more widely?) in AI Value Chain?)

### Navigating Governance Paradigms: A Cross-Regional Comparative Study of Generative AI Governance Processes & Principles

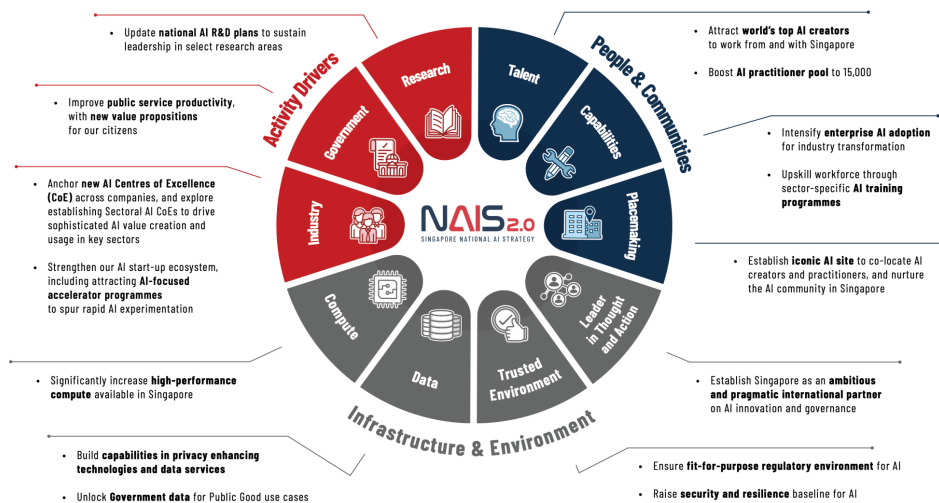
Jose Luna, Ivan Tan, Xiaofei Xie, Lingxiao Jiang  
 Singapore Management University  
 jose.luis.lc.2023@phdcs.smu.edu.sg, ivan.tan@smu.edu.sg, xfxie@smu.edu.sg, lxjiang@smu.edu.sg

H-GenAIGF: Processes, Principles & Cross-regional Coverage								
Constituent	Processes	Sub-Processes	SG	CN	EU	USA	UK	CA
DATA	Data Acquisition <sup>A</sup>	Data Sourcing <sup>T,F,P</sup>	-	✓	✓	✓	-	-
		Obtaining Consent <sup>T,P</sup>	X	✓	✓	✓	X	X
	Data Preparation <sup>A</sup>	Annotating & Labelling <sup>T,I</sup>	✓	✓	✓	✓	X	X
		Data Cleaning <sup>T,I</sup>	✓	✓	✓	X	X	X
	Storing & Sharing data <sup>S</sup>	Store	X	X	X	X	X	X
Share <sup>I</sup>		X	✓	✓	✓	X	X	
MODEL	Model Development <sup>I,A,S</sup>	Sourcing Models <sup>I</sup>	X	✓	✓	X	X	X
		Disclosing Infrastructure & Architecture <sup>T</sup>	-	X	✓	✓	-	X
	Model Validation & Testing <sup>T,F,A</sup>	Context Testing	✓	X	X	✓	X	✓
		Adversarial Testing	✓	X	✓	✓	-	✓
		Safety & Performance Benchmarking	✓	X	X	✓	X	X
		Preventing/Identifying Adversarial Attacks	✓	X	✓	✓	X	✓
	Model Deployment <sup>A,In</sup>	Distributing method	X	X	✓	✓	X	X
	Model Maintenance <sup>A</sup>	Operational Integration	X	X	✓	✓	X	X
Context Risk Analysis		✓	X	✓	✓	X	X	
Compliance & Risk Analysis <sup>A</sup>	Incident Reporting	X	X	✓	✓	X	X	
CONTENT GENERATION	Content Validation & Moderation <sup>I</sup>	Assessing & Mitigating Toxicity	✓	X	X	X	-	X
		Verifying Content Provenance	✓	X	✓	✓	X	✓
		Labeling Generated Content <sup>T</sup>	X	✓	✓	✓	-	✓
		Managing & Mitigating of Unlawful Content <sup>I</sup>	X	✓	✓	✓	X	X
	Managing Distribution & Access control <sup>F</sup>	Protecting Against Unlawful Content <sup>F</sup>	✓	X	✓	✓	-	X
		Providing Content Disclaimers	X	X	✓	✓	X	✓
Disclosure <sup>T</sup>	Detecting GenAI Content	✓	X	✓	✓	-	✓	
Feedback <sup>I,R</sup>		X	✓	✓	✓	-	X	
ETHICS	Ethical Alignment & Human Rights <sup>F</sup>	Ensuring Accountability & Responsibility throughout the Lifecycle <sup>Ac</sup>	✓	-	-	-	X	-
		Maintaining Sustainability & Environmental Responsibility <sup>S</sup>	✓	X	✓	✓	✓	X
	Upholding User Rights & Control <sup>P</sup>		X	X	✓	X	X	X

Principles:  
 T= Transparency      Ac=Accountability      S= Sustainability  
 F= Fairness          A= Auditability          P= Privacy  
 I= Integrity          In= Interoperability      R= Responsiveness

### Harnessing AI for the public good

Our second National AI Strategy, or NAIS 2.0, outlines our vision for Singapore to be a place where AI serves as a force for good, and where we harness AI to uplift and empower our people and businesses. To achieve our vision and goals, we will direct efforts under NAIS 2.0 toward 3 Systems, working through 10 Enablers.



## Governance Principles and Instruments

- **IMDA Model Framework:** Voluntary guidance for ethical AI design and deployment.
  - Launched by the Infocomm Media Development Authority (IMDA) in 2019, with a second version released in 2020.
  - Objective: Provide practical, voluntary guidance for private sector organizations on ethical and governance aspects of AI design and deployment.
  - Key Principles: (1) AI used in decision-making should be **transparent, explainable, and fair**; (2) AI solutions should prioritize “human-centric” values.
  - Updates in the Second Version (2020)
    - Internal AI governance
    - Human involvement in AI decisions
    - Operations Management
    - Stakeholder interaction

## AI Verify and Industry Engagement

- **AI Verify Toolkit:** Practical tools for testing and evaluation within organizations. “Audit by any other name?”
  - **AI Verify Foundation:** Global open-source community developing governance standards.
- **Government and Industry Collaboration:** Building a trusted AI ecosystem through active partnerships with businesses and international organizations.
- **Role of Standards in AI Governance**
  - Technical vs Governance standards?
  - Challenges of “encoding” normative governance principles into product (model and/or engineering stack)
  - What role for State and Market? (Background of industrial policy and critical industry regulation)



## Specific AI Governance Initiatives

- **Sector-Specific: Monetary Authority of Singapore (MAS)**
  - **FEAT Principles:** Fairness, Ethics, Accountability, and Transparency in AI use in the financial sector.
  - **Veritas Toolkit:** Assessment methodologies for fairness, ethics, and transparency.
- **Technology Specific: Generative AI Governance:** Details “dimensions” for governing generative AI, including content provenance, safety, and AI for public good.
  - Accountability, Data, Trusted Development and Deployment, Incident Reporting, Testing and Assurance, Security, Content Provenance, Safety and Alignment Research and Development, and AI for Public Good
  - Role for Technological Tools (eg, Privacy enhancing technologies, Input Moderation tools, Digital forensic tools)
  - (Why a separate Framework?)

## International and Regional Influence

- **ASEAN AI Governance Influence:**
  - **ASEAN Guide on AI Governance and Ethics:** Broad alignment with Singapore’s AI governance principles.
  - **Singapore’s Role in Shaping Regional AI Strategy:** Bridging gaps between ASEAN member states and promoting AI governance interoperability.
- **Global Leadership:** Participation in international AI governance forums (e.g., WEF, GPAI).



## Future Outlook: AI Governance in Singapore

### ■ Evolving Governance Approach:

- **Soft-Touch Regulation with Potential for Harder Regulation:** Singapore's capacity to shift toward more formal AI regulation if necessary.
- Preference for risk-and-principles approach; sectoral and technology-specific guidance where deemed necessary.
- **Technological Adaptability:** Ongoing updates to governance frameworks in response to emerging technologies.
- **Public Trust and Collaboration:** Sustained emphasis on building AI literacy and trust among citizens, ensuring responsible AI adoption. (Reflects attitudes and beliefs about role of state vs market and importance of AI to society and economy as well as geopolitical "elephant in the room"?)

...

## Data Protection, Competition, and AI Governance: The Importance of Data Portability and ADM Governance in Data Protection Laws



Qing HE

Assistant Professor, Beijing University of Posts and Telecommunications, China



### BIOGRAPHY



Dr. Qing He is an Assistant Professor in the Law Faculty at Beijing University of Posts and Telecommunications, China. She specializes in competition law and Internet law and holds a PhD in economic law. Her teaching and research interests include data protection, technology regulation, economic analysis of law, and comparative law.

Dr. He's recent work includes "Rethinking the Legal Regulation of Internet Platform Monopoly in China" (P&I, 2022), which is based on her conference paper presented at the Internet Governance Forum (IGF) 2021 – WS #77, focusing on antitrust regulation of Internet platforms from a global perspective. Her other recent publication, "Refresh the Reasonable Expectation: The Key to the Modern Privacy Rules" (Journal of Internet Law, 2023), explores data portability and individual autonomy, drawing on legal practices in the US, EU, and China. Additionally, Dr. He presented her work, "How Far Are We from Reaching a Consensus: China's Governance of ADM in Global Context," at the 21st Chinese Internet Research Conference (CIRC 2024).

# Abstract

Section I discusses the negative impact of data use policies on competition. Despite some positive effects on competition, the implementation of data transfer policies, such as the interoperability required for the exercise of data portability rights, is still flawed in promoting competition in certain respects.

Section II examines how ADM (Automated Decision-Making) governance influences AI governance. According to data protection laws in China and the EU, individuals have the right to object to decisions made by algorithms if the decision significantly affects them, which has implications for AI governance mechanisms.

This section focuses on three key aspects: (i) legal definitions, (ii) hierarchical and categorical protection policies, and (iii) liability rules. The presentation compares policies on ADM governance across the EU, the U.S., and China. For example, it explores the definition and scope of automated decision-making and its impact on individual rights, as well as the differences in ADM and Generative AI governance between the EU's AI Act, the U.S.'s Blueprint for an AI Bill of Rights, Biden's Executive Order, and China's Personal Information Protection Law (2021), Provisions on the Administration of Algorithm-generated Recommendations for Internet Services (2021), and Measures for the Administration of Generative AI Services (Consultation Paper, 2023), among others.

Section III highlights the significance of classifying risks in AI systems. This section focuses on legal practices in China, using three scenarios as examples: (i) financial systems (with a particular focus on credit scoring systems), (ii) price discrimination in online service systems, and (iii) employment-related systems (specifically electronic workplace surveillance and management systems).

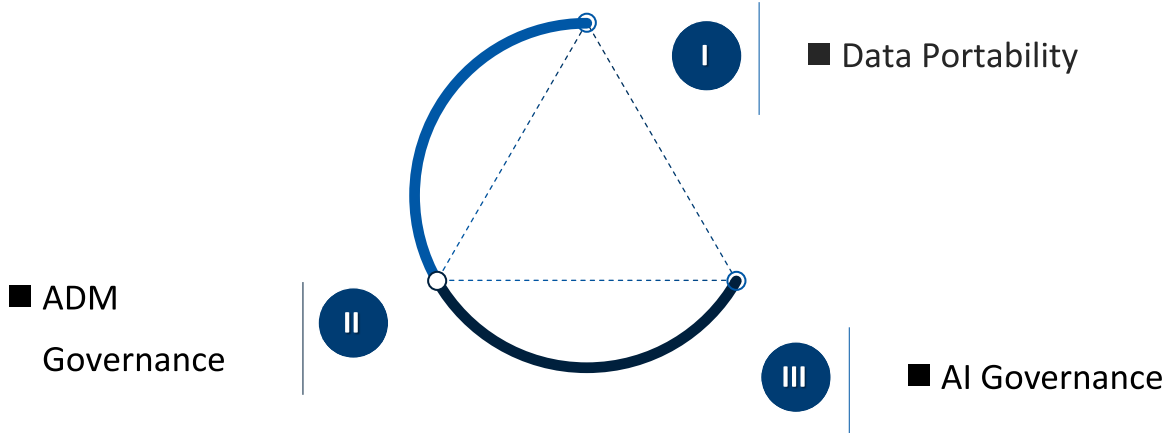


# Data Protection, Competition, and AI Governance: The Importance of Data Portability and ADM Governance in Data Protection Laws



Qing HE BUPT

## Data Protection Laws





## Contents

- I **Impact of data use policies on competition**
- II **Paradigm for ADM governance**
  - ✓ Legal definition
  - ✓ ‘3R’: Risk, Right, Responsibility
  - ✓ Legal practices in China
- III **Concluding remarks**

APB 2024



## Impact of data use policies on competition

- **The "open standard format" for implementing Data Portability**
- **Privacy protection requirement**
- **"Walled garden" problems**

APB 2024



## Paradigm for ADM governance: Comparative perspective

- **Legal definition**

---

- **Hierarchical and categorical protection policies**

---

- **Classifying risks of AI systems**

## Legal definition

APB 2024



### EU: GDPR

Art.22.1 Automated decision-making

The data subject shall have the right not to be subject to a decision based solely on automated processing, **including profiling**, which produces legal effects concerning him or her or similarly significantly affects him or her.



### China: PIPL

Art.73(2) Automated decision-making

the activity of using computer programs to automatically analyze or assess **personal behaviors, habits, interests, or hobbies, or financial, health, credit, or other status**, and make decisions.

**EU**

**ADM > Profiling**

**CHINA**

**ADM ≈ Profiling**

**What behaviors  
fall outside  
profiling?**



**EU: GDPR**

Art.22.1 Automated decision-making

Defining the  
**'major influence'**

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly **significantly affects** him or her.



**China: PIPL**

Art.24.3 Automated decision-making

When the use of automated decision-making produces decisions with a **major influence** on the rights and interests of the individual, .....they have the right to refuse that personal information handlers make decisions solely through automated decision-making methods.



**EU: GDPR**

Art.22.1 Automated decision-making

Proof of harms?

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly **significantly affects** him or her.



**China: PIPL**

Art.24.3 Automated decision-making

When the use of automated decision-making produces decisions with a **major influence** on the rights and interests of the individual, .....they have the right to refuse that personal information handlers make decisions solely through automated decision-making methods.



**EU: GDPR**

Art.22.1 Automated decision-making

Ex-ante regulation:  
**RISK**

The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly **significantly affects** him or her.



**China: PIPL**

Art.24.3 Automated decision-making

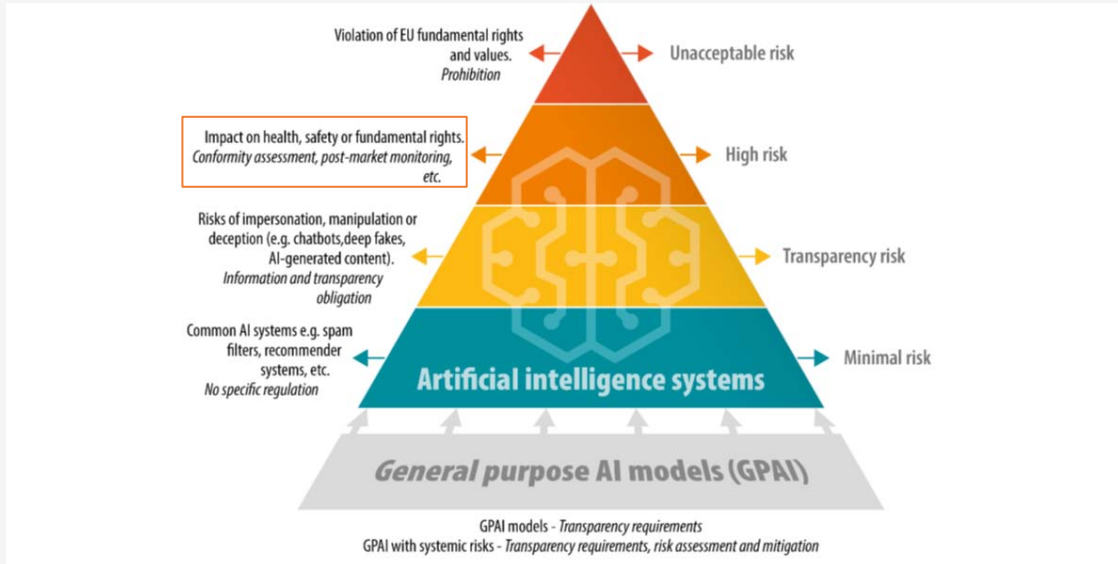
When the use of automated decision-making produces decisions with a **major influence** on the rights and interests of the individual, .....they have the right to refuse that personal information handlers make decisions solely through automated decision-making methods.

## Paradigm for ADM governance

*ADM-related policies in China, EU and US*

	CHINA	EU	US
<b>Legal definition</b>	ADM~Profiling	ADM > Profiling	ADM > Profiling
	Major influence	Significantly affect	Significant risk
<b>Hierarchical and categorical protection policies</b>	Sensitive PI	Special Categories of PI	Sensitive PI
	Severity of damage	Risk classification	Rights-based
<b>Liability rules</b>	Registration	Documentation	Documentation
	Transparency	Transparency	Transparency
	Explainability	Explainability	Explainability, interpretability

**EU AI Act**



Data source: EC

➤ **US: Blueprint for an AI bill of rights**

- Civil rights, civil liberties, or privacy;
- Equal opportunities;
- Access to critical resources and services

Rights-based ↔ Risk-based



Risk classification

'major influence'

APB 2024



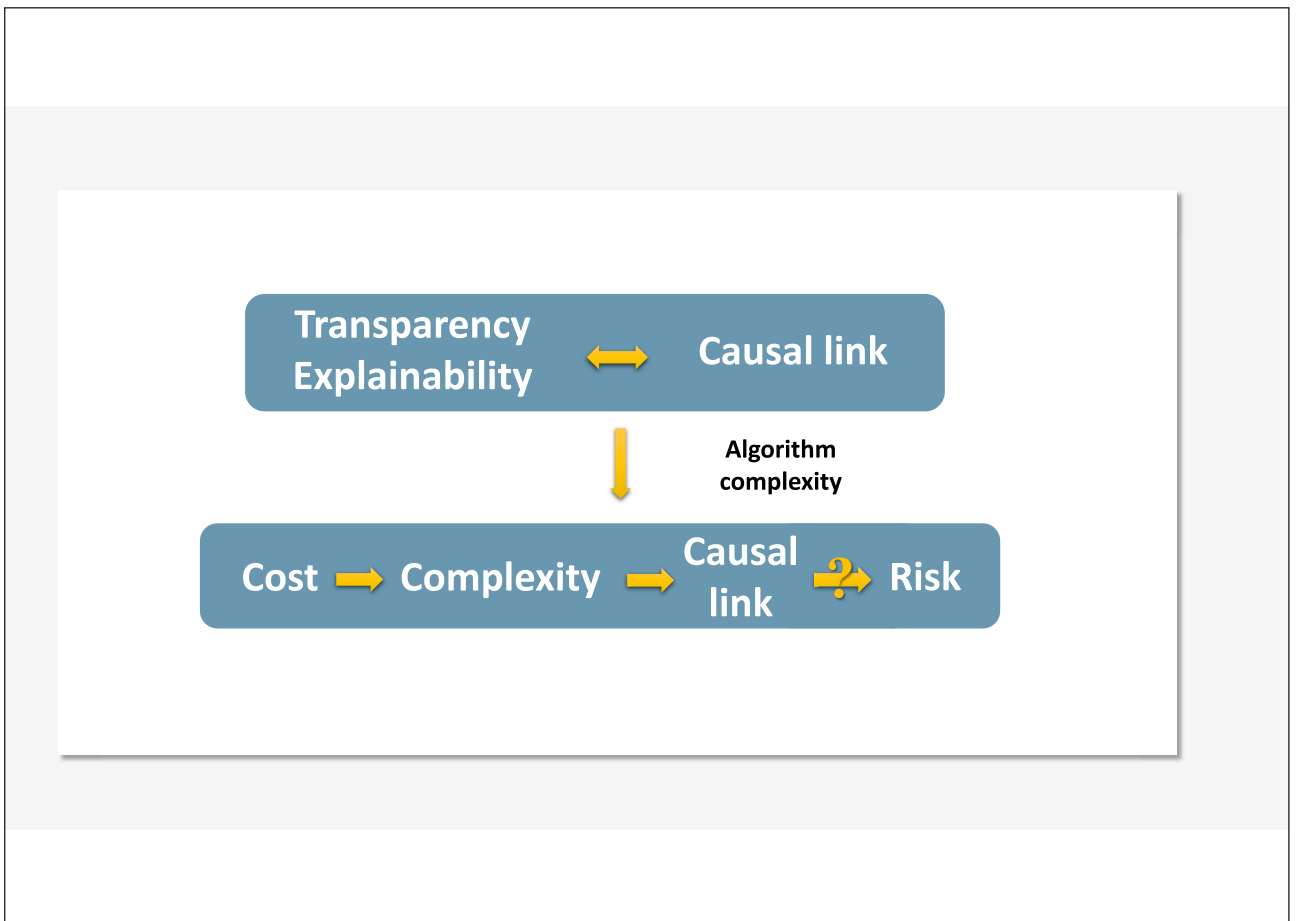
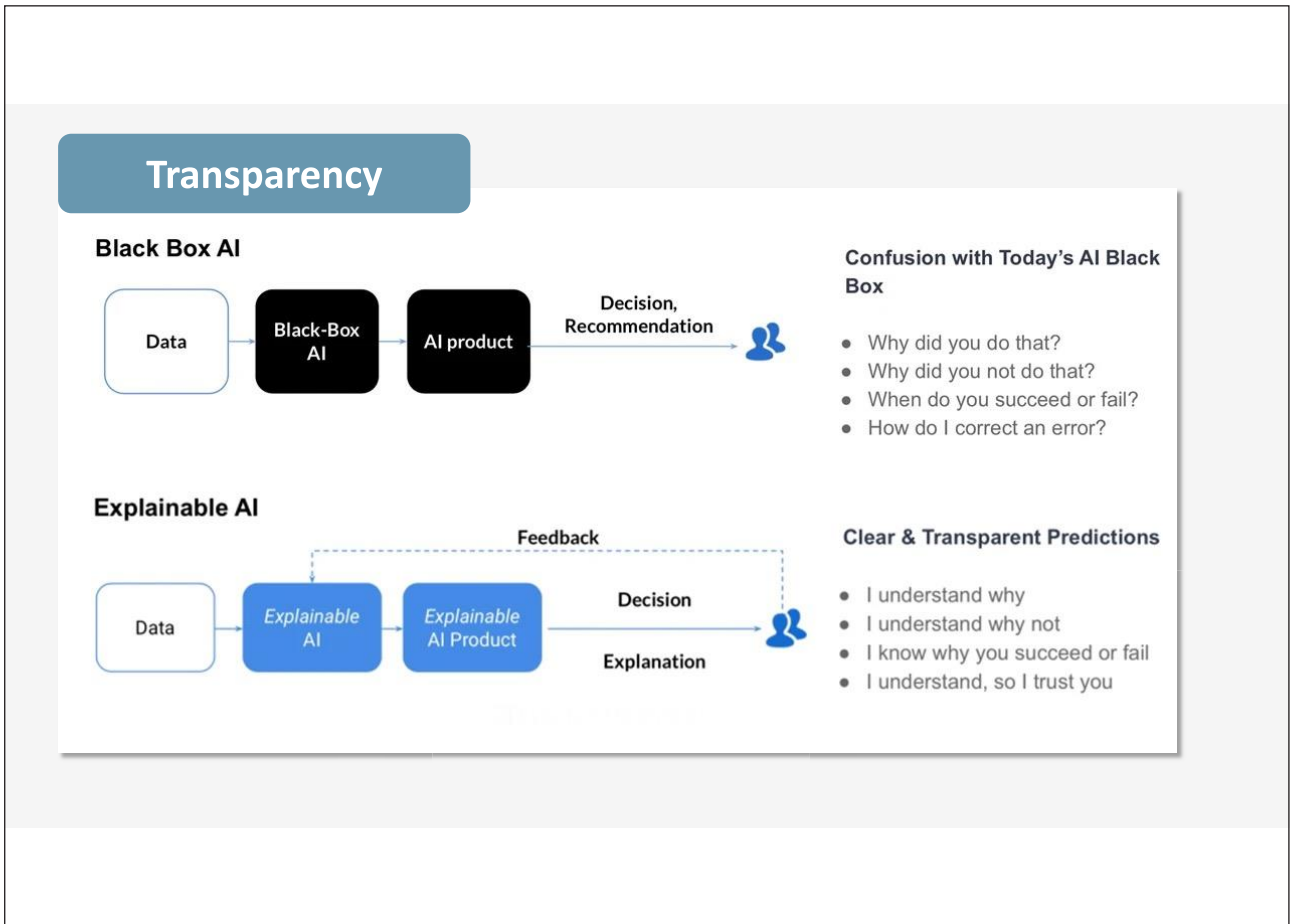
## Classifying risks of AI systems

- '3R': Risk, Right, Responsibility

**What is the relationship between risk and responsibility?**

- Legal practices in China





APB 2024



## Classifying risks of AI systems

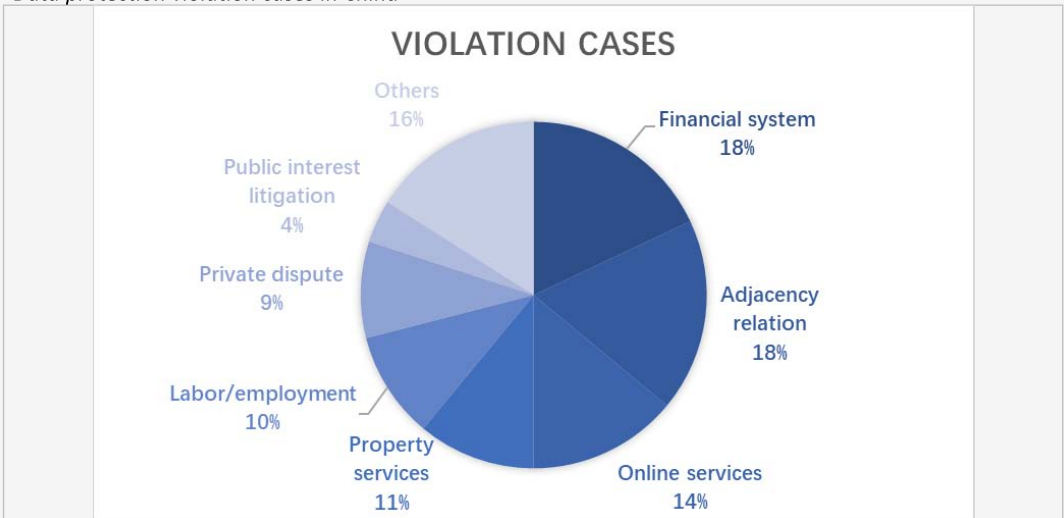
- '3R': Risk, Right, Responsibility

What is the relationship between risk and responsibility?

- **Legal practices in China**

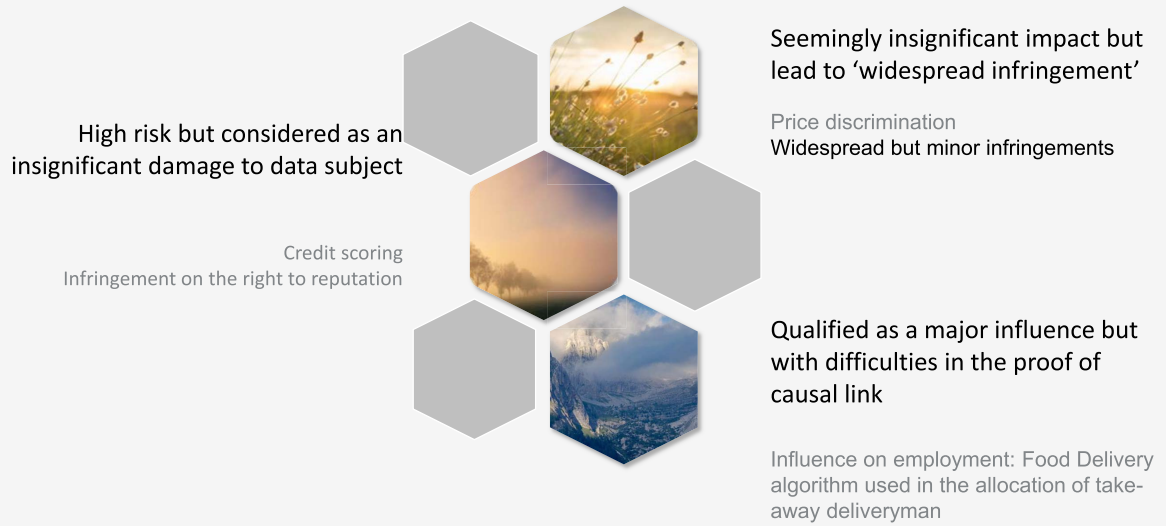
## Legal practices in China

Data protection violation cases in China



Nov. 1, 2021 - Oct. 23, 2023

## Legal practices in China







## Designing Accountable Community in the Emerging AI period



**Kohei Kurihara**  
CEO, Privacy by Design Lab, Japan



### BIOGRAPHY



Kohei is the Co-Founder of Privacy by Design Lab, a leading data privacy culture and society community. As a non-profit organization, Privacy by Design Lab was originally established as a privacy-oriented corporate structure program and policymaking initiative. We collaborate with multiple stakeholders, including public affairs, government, companies, civic organizations, and international watchdogs to enhance fundamental privacy culture. He has spoken at numerous international conferences, such as UNESCO, and participated in open-source projects as a data privacy and blockchain expert. He also has extensive experience in education and non-profit organizations, and has worked with secretaries of local politicians around the world to create and develop public policy.

# Abstract

This presentation focuses on delivering key insights to the design community and emphasizing accountability in the process of developing AI services and products. In line with the emerging AI trend in society, AI developers and providers are increasingly expected to take on responsibility, especially as regulatory and societal demands on the supply side rise in the coming decades.

To address this challenging theme, the discussion highlights the crucial role the design community plays in enhancing safety and accountability in relationships between diverse stakeholders. Additionally, by sharing effective knowledge and experiences, the community can prevent unexpected consequences by integrating different perspectives and insights early in the process.

The community comprises various experts and practitioners, deepening mutual literacy and occasionally leveraging their work through "connecting the dots" via project collaborations. These projects strengthen the trusted networks among parties that share a similar vision, contributing to the community's goals.

These are the main topics in this presentation. The necessary action in the emerging AI period to prevent the unexpected consequences Multi-stakeholder based accountability model by sharing diverse experiences and methods Learning and Sharing community function to leverage community member synergies in the projects Designing the vision and roadmaps with diverse backgrounds beyond the cultures and histories Finding the remarks of community benefits against the AI harms As a conclusion, the presenter will show future affection with community based authentic relationship building from his past methodology and containing the actionable planning to design community network. And he will speak about the future community design to boost the designing opportunities in multilateral Asian approaches.

# Designing Accountable Community in the Emerging AI Period

© 2024 Privacy by Design Lab

1

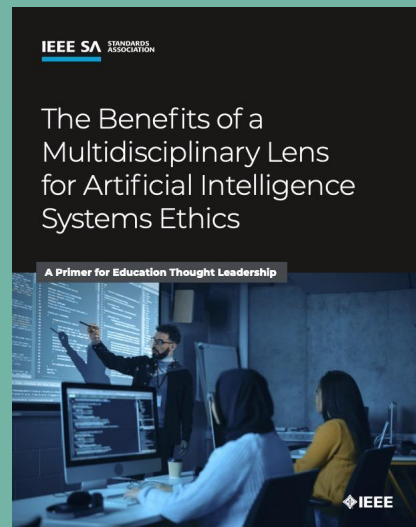
## Introduction



**Kurihara Kohei**  
Privacy by Design Lab

Kohei is Co-Founder of Privacy by Design Lab, a leading data privacy culture and society community. As a not-for-profit, the organization was originally established as a privacy oriented corporate structure program and policymaking. We collaborate with multi-stakeholders, public affairs, government, companies and civic organizations, and international watchdogs to enhance fundamental privacy culture. He has spoken at many international conferences such as UNESCO and participated in open-source projects as a data privacy and blockchain expert. He also has extensive experience with education and non-profit organizations, and working with the secretaries of local politicians around the world creating and developing public policy.

© 2024 Privacy by Design Lab



2

## Table of Contents

What is Privacy by Design Lab?

What is AI and accountability initiatives in Japan?

How can we implement the Privacy by Design in AI period?

Q&A

© 2024 Privacy by Design Lab

3

## What is Privacy by Design Lab?

Privacy by Design was established by four voluntary members to promote the awareness of privacy by design in our society. Two members are remaining to lead the societal initiative for our future development.



Initial founding members took our memory at the front of Tokyo legal affairs bureau. Two members have left the company, but they are leading own journey.



Privacy by Design cooperates with industry leaders to encourage private companies to design their privacy practices.

© 2024 Privacy by Design Lab

4

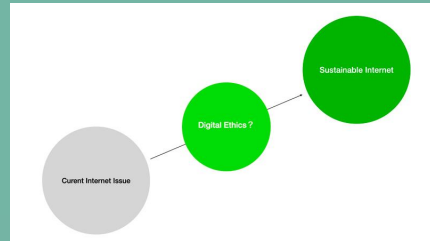


## What is Privacy by Design Lab?

Holding the "Privacy by Design Conference" once in a January to celebrate the data privacy and data protection day with different stakeholders.



At the conference, we invite different stakeholders such as the government, international organizations, private sectors, human right organizations and more.



In this year, we discuss "digital ethics" for the future sustainable internet. Our main topic is gathering different stakeholders to have a dialogue for the future.

## What is AI and accountability initiatives in Japan?

# What is AI and accountability initiatives in Japan?

Japanese Ministry of Economy, Trade and Industry released AI guidelines for business in this April, with Ministry of Internal Affairs and Communications.

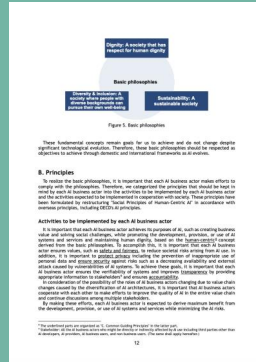
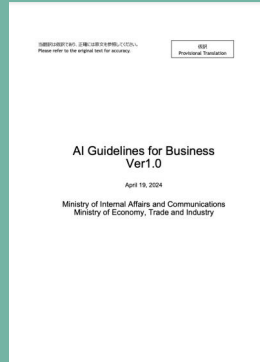
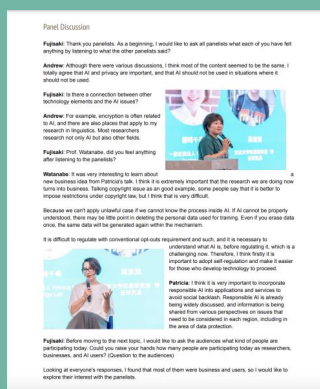
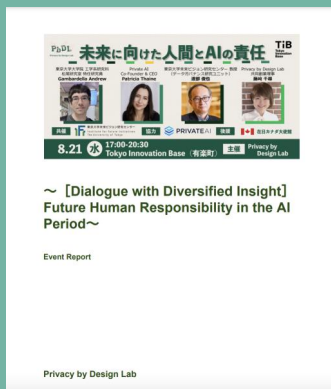


image: AI Guidelines for Business Ver.1.0

# What is AI and accountability initiatives in Japan?

At our latest event with Tokyo University, the speakers and panelists speaks about Japanese AI and responsibility trend for the audiences.



## What is AI and accountability initiatives in Japan?

Learning from Japanese local community, I summarizes the essences of the perception  
"AI accountability" with basic three pillars.

Demand Clear  
Threshold

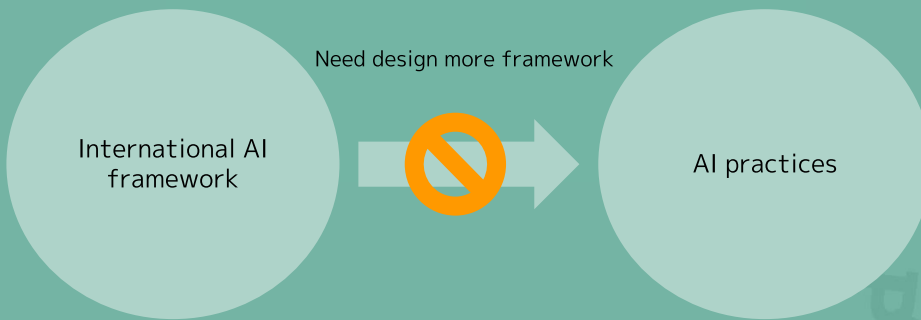
Need More Social  
Context

Soft-Law based  
Voluntary Approach

## How can we implement the Privacy by Design in AI period?

## How can we implement the Privacy by Design in AI period?

At the current international framework and models highly rely on "consensus model" among multi-stakeholders. It is also taking into account with "design", but highlight more consensus approach.

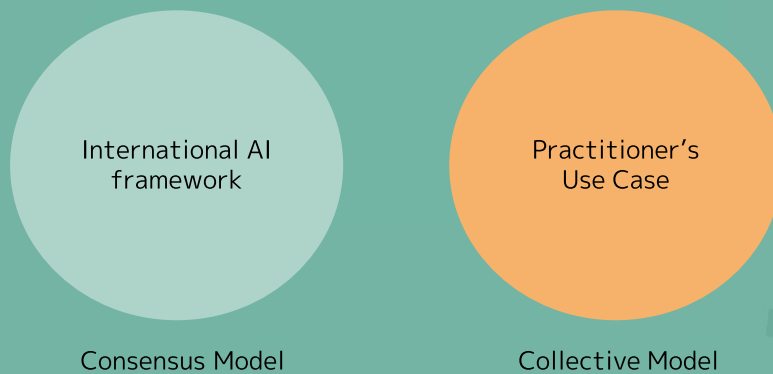


© 2024 Privacy by Design Lab

11

## How can we implement the Privacy by Design in AI period?

To implement the designed model in practice with multi stakeholders, "collective model" is more effective rather than "consensus model" for business practitioners to learn and practices.

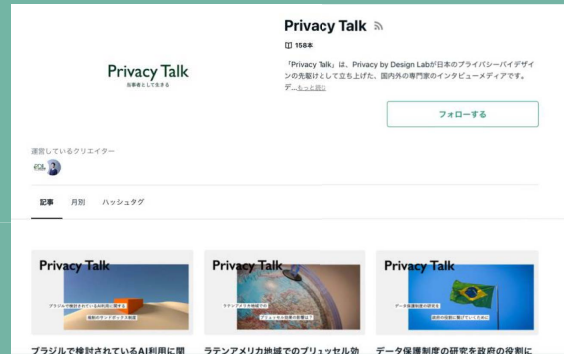
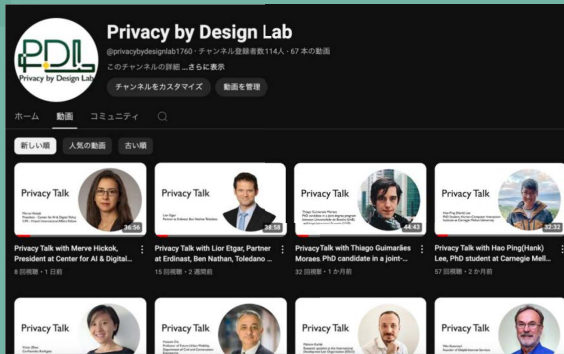


© 2024 Privacy by Design Lab

12

## How can we implement the Privacy by Design in AI period?

As a collective model example, we are running interview channel with privacy and human rights practitioners. This channel is the community among sharing experiences and knowledge as practical references in the AI period.

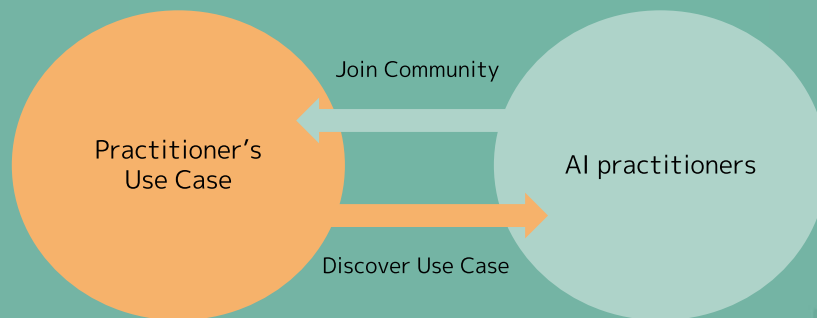


© 2024 Privacy by Design Lab

13

## How can we implement the Privacy by Design in AI period?

As a Japanese policy maker priorities **soft-law and voluntary governance** approach, and civil society and NGO will have different role from western countries, which is not only contributed to the consensus model, but collective method to increase the awareness and references for the practitioners.



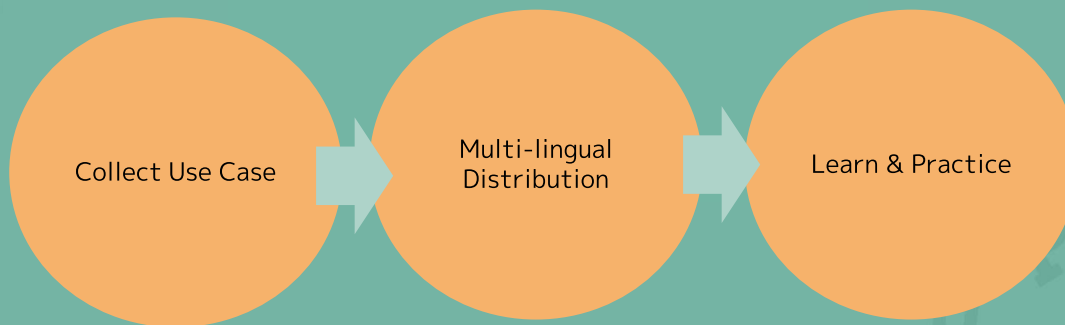
Voluntary Governance Flow

© 2024 Privacy by Design Lab

14

## How can we implement the Privacy by Design in AI period?

To implement the practices based on "collective model", we work for the interviews with practitioners and share their history and essences with multiple languages,



© 2024 Privacy by Design Lab

15

## How can we implement the Privacy by Design in AI period?

In this model, we have received the feedbacks and collaborative requests from multiple regulators. Practitioner's interview influences lawmakers to create the better society and awareness together.

### Talk with EDPS

Privacy Talk interview bridges our mission and European regulator to exchange mutual future roadmap to create new projects. Thanks to this opportunity, we had started our initiatives such as annual "Privacy by Design Conference" and they are one of our stakeholders.



Left, Leonardo, Fujisaki, Kurihara  
EDPS2022 @ Brussels, Belgium

### Talk with Taiwanese government

Privacy Talk influences the Taiwanese delegates to oversight future Taiwanese privacy environment. Interview contents clarify the ambiguous points of privacy and data protection contexts and inspire the different regional actors with their unknown backgrounds and insights.



Left, Chen, Yu, Morris, Vivian  
2024 @ Tokyo

© 2024 Privacy by Design Lab

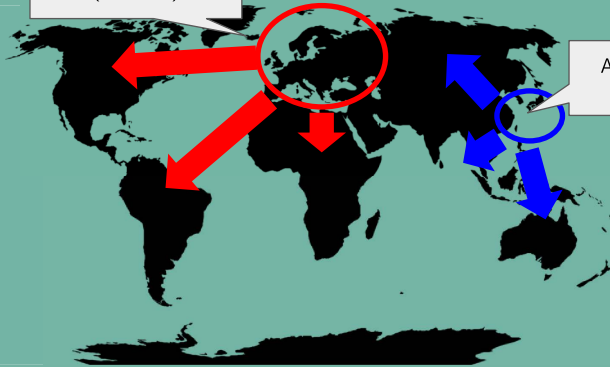
16

## How can we implement the Privacy by Design in AI period?

We work to expand interview community to the Asian region with local practices.  
We are pleased to discuss you to join us and design our privacy with "collective model".

※Establish an European gateway after the CDPD 2025 in Brussels to build the profound relationships with local privacy leaders

European Gateway  
(2025~)



Asian Gateway  
(2025.8~)

※Building the relationship with Taiwanese government after the commencement of Taiwanese Privacy Commissioner in 2025, Aug toward Asian landscape

## Q&A





Day  
**1**

# Session 2

## Reconciling Data Protection and Competition Laws in the Age of AI

### Chair

Ha Young Kim

Professor, Graduate School of Information,  
Yonsei University, Republic of Korea



### 1

Orla Lynskey

Professor, University College London,  
Law School, UK



### 2

Kunifumi SAITO

Associate Professor, Faculty of Policy Management,  
Keio University, Japan



### 3

Dae-Hee Lee

Professor, Korea University, Law School,  
Republic of Korea







## Taking Stock: Data Protection, Privacy, and Competition Law



Orla Lynskey

Professor, University College London, Law School, UK



### BIOGRAPHY



Professor Orla Lynskey holds a Chair in Law at Technology at UCL Laws and is a Visiting Professor at the College of Europe Bruges. She teaches and conducts research in the areas of data protection, data governance, fundamental rights and competition and regulation. Prior to joining UCL Laws, she was an Associate Professor at LSE Law School which she joined in 2012. She is joint Editor in Chief of International Data Privacy Law (Oxford University Press) and an Editor of the Modern Law Review. Orla regularly engages with policymakers and has given invited evidence to the British Houses of Parliament, the US FTC, the Global Privacy Assembly and the OECD, amongst others.

# Abstract

Data protection and competition law have historically been treated as distinct fields of law with clearly demarcated boundaries and there has been significant resistance to the breakdown of these boundaries. Nevertheless, legal and technical developments (such as Apple's use of a Privacy defence to defend allegations of abuse of market power) mean that their intersection is now inevitable. This presentation maps and critically analyses the four ways in which these areas of laws exert influence on one another. First, data protection law is not neutral – its application (or lack of application) affects market dynamics in a way that is relevant to competition law. Second, data protection is integrated into competition law analysis as part of the consumer welfare benchmark. Third, competition considerations influence the interpretation of some data protection concepts, such as consent, and the extent of data protection interferences. Finally, the legislature recognises this intersection by imposing limitations on the data processing activities of digital gatekeepers, subject to data protection law.

# TAKING STOCK: DATA PROTECTION, PRIVACY AND COMPETITION LAW

13<sup>th</sup> Asia Privacy Bridge Forum

Prof. Orla Lynskey - UCL Laws ([o.lynskey@ucl.ac.uk](mailto:o.lynskey@ucl.ac.uk))

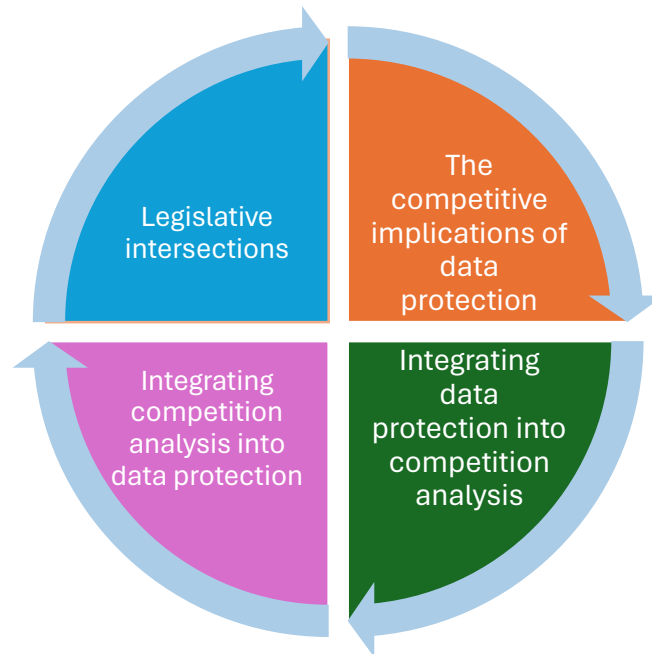
## HYPOTHESIS

Mutually impactful relationship between competition and data protection/privacy

- Points of coherence
- Tensions

Reflected in judicial, legislative and institutional developments

## FOUR POINTS OF INTERSECTION BETWEEN DATA PROTECTION AND COMPETITION



## THE COMPETITIVE IMPLICATIONS OF DATA PROTECTION

- Renders data sharing “impossible”
- Reduces incentives for data sharing
- Influences with whom you merge
- High costs of non-compliance (e.g., polluted data-sets)
- Uncertainty costs
- Trust effect on data subjects (household names)

*Gal and Aviv, 2020*

## THE COMPETITIVE IMPLICATIONS OF DATA PROTECTION: OBSERVATIONS

The enforcement of data protection legislation (or lack thereof) affects competitive dynamics

Assumption in competition law literature that data protection law displays a preference for first-party data “sharing” rather than third-party

Data protection law may have competitive “costs”: a societal cost of privacy

## COMPETITION ON DATA PROTECTION

Data protection law as a normative benchmark: recognised by EU Commission in *Microsoft/LinkedIn*

- Abusive exploitation on data use conditions
- ‘Predatory’ data protection policies?
- Agreement to restrict competition on data protection
- Non-compliance with data protection law as an indication of departure from ‘competition on the merits’

## **COMPETITION ON DATA PROTECTION META PLATFORMS – CJEU**



[Users of dominant services] **must be free to refuse individually [...]** to give their consent to particular data processing operations not necessary for the performance of the contract, **without being obliged to refrain entirely from using the service offered by the online social network operator**, which means that those users are to be offered, if necessary for an appropriate fee, an equivalent alternative not accompanied by such data processing operations. [150]

## **COMPETITION ON THE MERITS : SUBSTANTIVE OBSERVATIONS**



Identifying qualitative criteria to assess *quality*

- Discretion in regulatory framework leaves scope for competition
- Global convergence around a core set of data privacy principles (Convention no.108; FIPPs)
- Data security; data accuracy; anonymization; data minimization; transparency.

Also: entrenches an individualistic approach to data protection law



## COMPETITION ON THE MERITS : INSTITUTIONAL OBSERVATIONS



Competence creep and possibility that competition authorities will “get there first” and interpret data protection through an economic lens

Role of civil society: do competition proceedings facilitate third party interventions on non-economic grounds?

What impact does this have on the role of private enforcement of data protection law?

## THE RELEVANCE OF COMPETITION TO DATA PROTECTION



Search engine enables any internet user to obtain a ‘structured overview’ of information relating to the individual, including ‘information which potentially concerns a vast number of aspects of his private life and which, without the search engine, could not have been interconnected or could have been only with great difficulty’ (*Google Spain*, [36-38])

‘Furthermore, the effect of the interference with those rights of the data subject is heightened on account of the important role played by the internet and search engines in modern society, which render the information contained in such a list of results ubiquitous...’ [80]

# LEGISLATIVE INTERSECTIONS: THE GDPR/DIGITAL MARKETS ACT

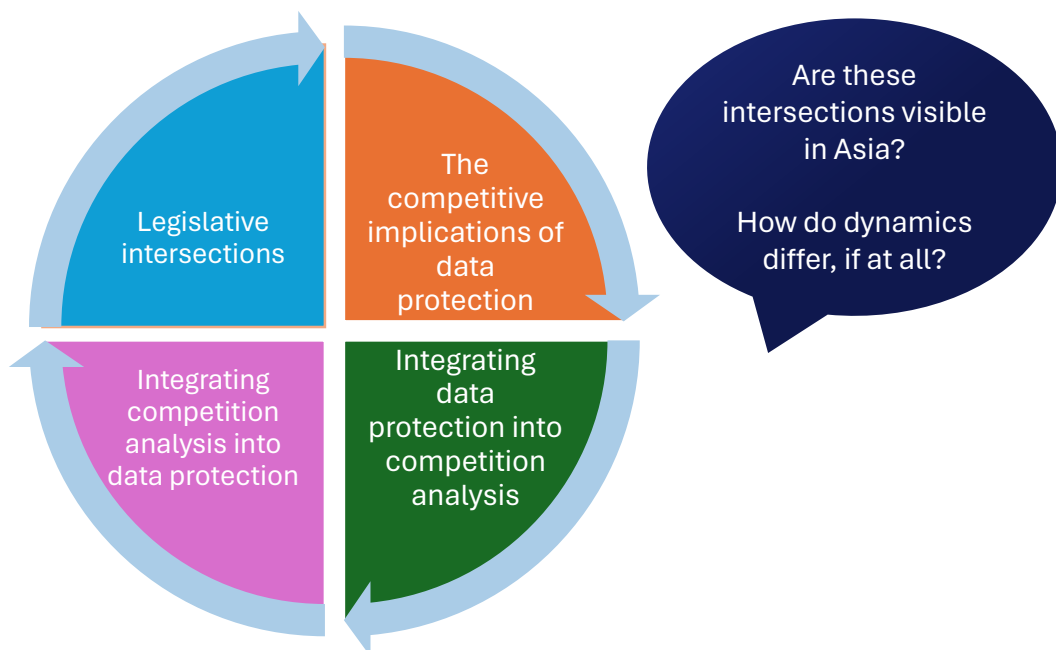
## Gatekeeper:

- Providing Core Platform Services
- Significant impact on the Internal Market
- Enjoys or will enjoy an entrenched and durable position

## Article 5: Obligations:

- A series of prohibitions relating to personal data: behavioural advertising; combination and cross-use of data; automated sign-ins to GK services
- BUT not applicable where end user has been provided with a specific choice and consents.

## FOUR POINTS OF INTERSECTION BETWEEN DATA PROTECTION AND COMPETITION





## Reproduction of Personas with AI and the Right of Publicity



Kunifumi SAITO

Associate Professor, Faculty of Policy Management,  
Keio University, Japan



### BIOGRAPHY



Kunifumi Saito is an Associate Professor in the Faculty of Policy Management at Keio University. He specializes in civil liberties and technology law. His current research interests include privacy and data governance. He received a Ph.D. in Media and Governance from Keio University and a J.D. with summa cum laude honors from Waseda Law School. He is a member of the Daini Tokyo Bar Association and practiced law at Jones Day in Tokyo. Prior to joining Keio University in 2017, he served as Deputy Director in the Japanese Government's Consumer Affairs Agency and as Senior Manager of the Information Systems Planning Department at Mitsubishi UFJ Financial Group. He is the vice-chairperson of the Privacy Mark System Committee of JIPDEC, the chair of the Business Law Study Group of the Information Network Law Association in Japan, and a member of the editorial board of the Japan Society of Information and Communication Research.

# Abstract

This presentation examines the relationship between the personality rights and the right of publicity in the context of the reproduction of personas using artificial intelligence.

In the United States, most lawyers consider the right of publicity to be a type of intellectual property right like copyright. Recently, however, an argument has emerged that emphasizes the similarities with the right to privacy. It classifies the functions of the right into four categories: the Right of Performance, the Right of Commercial Value, the Right of Control, and the Right of Dignity. It is significant that the similarity between the Right of Commercial Value, which is the core of the function, and the trademark right has been pointed out.

Meanwhile, in 2012, the Japanese Supreme Court positioned the right of publicity as a kind of personality right. However, the official commentary to the decision emphasizes the similarities between the right of publicity and copyright. And in practice, disputes over the right of publicity are assigned to the specialized divisions for intellectual property of the courts. In addition, the case law of the lower courts distinguishes between the right of publicity and the rights of personality that relate to moral damages, such as the right of privacy and the right of likeness.

Under Japanese law, personal rights cannot be inherited. For this reason, it is believed that a celebrity's right of publicity also ceases upon his or her death. In this presentation, we will examine the legal rights involved in the reproduction of the persona of the deceased using artificial intelligence. In our discussion, we will draw on a theory from the United States that focuses on the similarities between the right of publicity and trademark law.

The 13th Asia Privacy Bridge Forum 2024

## Reproduction of Personas with AI and the Right of Publicity

---

Kunifumi SAITO, Ph.D.  
Keio University, Japan

Keio University Global Research Institute



---

## THE RIGHT OF PUBLICITY UNDER JAPANESE CASE LAW

Keio University Global Research Institute



## Supreme Court of Japan - Pink Lady v. Kobunsha (2012)

- ✓ Since a person's name and portrait are symbols of his personality, that person has the right not to have them used without good reason, as a derivative of his right to personal dignity.
- ✓ Since **the right of publicity**, which is the right to make exclusive use of such customer attraction, is based on the commercial value of the portrait itself, it constitutes **an aspect of the rights derived from the above-mentioned right of personality.**

## Supreme Court of Japan - Pink Lady v. Kobunsha (2012)

- ✓ Unauthorized use of the portrait constitutes **a violation of the right of publicity** under tort law if it is done **for the sole purpose of exploiting the customer appeal** of the Portrait, such as
- ✓ [1] Using the portrait as products that can be independently appreciated,
- ✓ [2] attaching the portrait to products for the purpose of differentiating the products, or
- ✓ [3] using the portrait to advertise products.

## Official Commentary for the Supreme Court Decision

- ✓ This ruling is clearly in favor of the theory that the right of publicity is **a derivative of the right of personality**.
- ✓ Although the right of publicity is related to the right of personality, which is like the umbilical cord, this judgment has clarified that it is positioned as **an intellectual property right** to protect economic interests in terms of case law.
- ✓ Although the right of publicity is derived from the right of personality, it is **a form of property right** that protects economic assets that are **different from the rights of dignity**, because it is the right that is composed by extracting and purifying the commercial value of portraits.

---

## THE RIGHT OF PUBLICITY IN THE UNITED STATES

## Supreme Court of the US - Zacchini Case (1977)

- ✓ By contrast, the State's interest in permitting a "right of publicity" is in **protecting the proprietary interest** of the individual in his act in part to encourage such entertainment.
- ✓ As we later note, the State's interest is **closely analogous to the goals of patent and copyright law**, focusing on the right of the individual to reap the reward of his endeavors and having little to do with protecting feelings or reputation.

## Taxonomy of the Right(s) of Publicity

- ✓ Post & Rothman (2020)
  - i. The Right of Performance
    - Zacchini v. Scripps-Howard Broadcasting Co.
  - ii. **The Right of Commercial Value**
    - Confusion, Diminishment and Unjust Enrichment
  - iii. The Right of Control
    - Autonomous Self-definition (Recht auf informationelle Selbstbestimmung)
  - iv. **The Right of Dignity**
    - Civility: against Highly Offensive Use



---

## REPRODUCTION OF PERSONAS WITH AI

Keio University Global Research Institute



### AI Hibari Misora (2019)

---

- ✓ Until her passing in 1989, Hibari Misora recorded over 1500 songs, leaving behind a series of hits in her more than 40 year long career as Japan's top singer.
- ✓ She posthumously became the first female recipient of the People's Honor Award, one of the highest honors in Japan.



- [https://archive.yamaha.com/en/news\\_release/2019/19100801/](https://archive.yamaha.com/en/news_release/2019/19100801/)

Keio University Global Research Institute



## Confusion-based Theory of the Right of Publicity

- ✓ Lemley (2019)
- A confusion-based theory of the right of publicity might also do a better job of preventing zombie rights of publicity.
- ✓ Dogan & Lemley (2006)
- We can imagine only limited circumstances in which a confusion-based right of publicity might survive death, such as **the use of digital technology to make it seem that an actor appeared in a movie in which he did not.**

## Personality-based Theory of the Right of Publicity

- ✓ Rothman (2012)
- In the context of publicity rights, it may be appropriate to permit heirs and beneficiaries (and the decedent) to limit some uses of the deceased's identity, at least in the aftermath of the death.
- The risk that survivors might violate the wishes of the deceased is an acceptable risk, however, because a postmortem right provides **the tools to prevent forced commodification against the wishes of the deceased and her heirs,** even if those tools are not always used.

## References

---

- ✓ Stacey L. Dogan & Mark A. Lemley, What the Right of Publicity Can Learn From Trademark Law, 58 Stan. L. Rev. 1161 (2006).
- ✓ Jennifer E. Rothman, The Inalienable Right of Publicity, 101 Geo. L. J. 185 (2012)
- ✓ Mark A. Lemley, Privacy, Property, and Publicity, 117 Mich. L. Rev. 1153 (2019).
- ✓ Robert C. Post & Jennifer E. Rothman, The First Amendment and the Right(s) of Publicity, 130 Yale L. J. 86 (2020)





## Personal Data & Generative AI



Dae-Hee Lee

Professor, Korea University, Law School, Republic of Korea



### BIOGRAPHY



Dae-Hee Lee is a Professor of Law at Korea University School of Law, specializing in Information Technology Law and intellectual property. He holds a Doctor of Juridical Science (S.J.D.) from the University of Wisconsin, Madison, where he also earned his LL.M. and M.L.I. degrees. Additionally, he holds a Master of Law and a Bachelor of Law from Korea University. Professor Lee has been a WIPO Domain Name Panelist since 2008 and a licensed attorney in New York since 2000. He serves as a mediator for the Internet Address Dispute Resolution Committee and the Seoul Central District Court. He is also a director at Creative Commons Korea and editor-in-chief of a quarterly publication on copyright. His expertise in copyright and IT law has made him a prominent figure in both South Korea and international legal circles.

# Abstract

The presentation addresses Korea's personal data regime and its related issues concerning AI development. Specifically, it focuses on the recently released "Guidelines on Processing of Personal Information Publicly Available for the Development and Deployment of AI Models" by Korea's Personal Data Protection Commission. The presentation argues that personal data concerns should not serve as obstacles to AI development.

# Lawful Basis for Processing Publicly Known Personal Data in the Age of AI

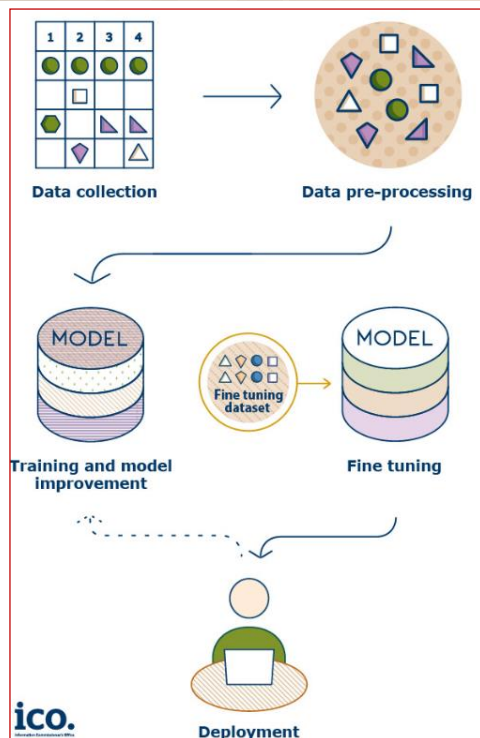
Reconciling Data Privacy and Competition Law in the Age of AI  
Asia Privacy Bridge Forum

Barun ICT Research Center

Oct. 17, 2024

Dae-Hee Lee  
Korea University School of Law

## AI Value Chain



- **Data collection** → **Pre-processing data** (Curation) → **Training** of AI model → (Pre-trained) **AI model** → Fine tuning/ Evaluation of performance → Deployment → Operation → End users → **Generation of AI outputs**

- **General-purpose AI model** → **Fine tuning** → **Deployment** (Licensing, Open AI, API) → Services provided → **Generation of AI outputs** by end users

## Processing Personal Data in AI Development

- **AI model:** An **algorithm** trained on a data set to perform a specific predictive task
- **AI model training:** Process of feeding the algorithm data, examining the results, and tweaking the model output to increase accuracy and efficacy
  - Needs **massive amounts of training data**
  - Included in training data are **personal data** (and copyrighted work)
- Most AI developers are dependent upon **publicly accessible sources for their training** (**internet**)
  - How? → Web scraping
- **Web scraping** → S/W(crawler) crawls web pages, gathers, copies and/or extract information, and store the information
  - **All related to processing of personal data**
- **Lawful processing of personal data** needs to be met in all stages of AI development, in particular in **data collection**
- **Balance** needs to be struck between **protection of personal data** and **promotion AI innovation**
  - Publicly available personal data

### Personal data considerations in AI stages of development and use

- (i) Collection of training data (including the use of web scraping data or reuse of datasets)
- (ii) Pre-processing of the data (including filtering)
- (iii) Training
- (iv) Prompts and AI output
- (v) Training AI with prompts

## Personal Data Considerations in AI

### 1. Lawful basis

- The traditional notion of "**consent**" is no longer a viable proposition in the context of an algorithmic society.
2. Transparency
  3. Data subject rights
  4. Data minimization
  5. Storage limitation
  6. Privacy by design
  7. Special category data



## Lawfulness of Processing: GDPR

### Art. 6 Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

- (a) the data subject has given **consent** to the processing of his or her personal data for one or more specific purposes;
- (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
- (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
- (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
- (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
- (f) **processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party**, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

### Art. 9 Processing of special categories of personal data

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

- **Sensitive data**

2. Paragraph 1 shall not apply if one of the following applies:

...

## Lawfulness of Processing: Korea

### PIPC Article 15 (Collection and Use of Personal Information)

(1) A personal information controller may collect personal information in any of the following cases, and use it within the scope of the purpose of collection:

- 1. Where **consent** is obtained from a data subject;
- 2. Where special provisions exist in other statutes or it is unavoidable due to obligations under statutes or regulations;
- 3. Where it is unavoidable for a public institution's performance of work under its jurisdiction as prescribed by statutes or regulations, etc.;
- 4. Where it is necessary to take measures at the request of a data subject in the course of performing a contract concluded with the data subject or concluding a contract;
- 5. Where it is deemed manifestly necessary for the protection, from imminent danger, of life, bodily and property interests of a data subject or a third party;
- 6. **Where it is necessary to attain the legitimate interests of a personal information controller**, which such interest is manifestly superior to the rights of the data subject. In such cases, processing shall be allowed only to the extent the processing is substantially related to the legitimate interests of the personal information controller and does not go beyond a reasonable scope.
- 7. Where it is urgently necessary for the public safety and security, public health, etc.

...

## Italy Garante Decision: ChatGPT

### Provision of March 30, 2023 [9870832]

- [N]o information is provided to users or to the data subjects whose data has been collected by OpenAI, L.L.C. and processed through the ChatGPT service;
  - [\[L\]ack of a proper legal basis concerning the collection of personal data and its processing for the purpose of training the algorithms underlying the functioning of ChatGPT;](#)
  - [P]rocessing of personal data of users, including minors, and of data subjects whose data is used by the service, constitutes **a violation of Articles 5, 6, 8, 13, and 25** of the Regulation
- ...

## Legitimate Interests : UK

Is **legitimate interests** a valid lawful basis for **training generative AI models** on web-scraped data?

### Requirements (Korea)

1. Processor's legitimate interest
2. Necessity to achieve processor's legitimate interest
3. Data subject individuals' rights do not override processor's interest
4. Processing is substantially related to the legitimate interests of the personal information controller and does not go beyond a reasonable scope

## Guidelines from PIPC



- PIPC, **Guidelines on Processing Publicly Available Data for AI (July 17, 2024)**

- Guideline on use of public personal data
- Addressing legal uncertainties for AI companies & Enhancing privacy protection for citizens
- Outlines how AI companies can legitimately and safely process data that is openly accessible on the internet

- **Legal gray area in AI development**

1. Personal data
2. Copyright

safe and legal use of public data within the current regulatory system

## Legitimate Interests : Guidelines

### 1. Processor(AI developer)'s legitimate interests

- Encompass not only the **business interests** of AI developers and service providers but also the broader **social benefits that may arise from it**.

- **Societal interests**

1. **Enhancing the fairness of AI outputs** by ensuring that specific personal information is not excluded from AI training to prevent the generation of discriminatory predictions based on race, religion, region, gender, income, property, etc.
2. **Preventing the underperformance of AI** regarding specific languages due to undertraining on data presented in those languages, and **preventing reduced accessibility to AI** by individuals who use that particular languages

- In defining legitimate interests, both **social benefits and social costs** within a reasonably foreseeable scope should be considered

- **Social benefits:** Preventing monopolization and promoting technological innovation in various fields such as healthcare and education by allowing small and medium-sized enterprises (SMEs) with limited capital to freely use, modify, and distribute technology
- **Social costs:** Difficulty to correct or retrieve (open-source) AI model in case vulnerabilities related to privacy violations are discovered, and there is also a risk of malicious use (e.g., spreading false information).

## Legitimate Interests : Guidelines

### 1. Processor(AI developer)'s legitimate interests

- **Legitimate interests**

- Specified through the "purpose" intended to be achieved by processing personal data and is bound by the **principle of purpose specification**

- **Ex. of no legitimate interests**

1. Developing AI systems for **profiling and surveillance of individuals by combining with facial recognition databases**
2. Developing AI systems for purposes of **cyberattacks or identity theft fraud**

- **Task-specific AI v. General purpose AI**

#### 1 Task-specific AI

- Desirable to define the intended purpose and use of the AI as specifically as possible

#### 2. General-purpose AI

- Specified by using reasonably foreseeable AI system types, technically implementable functionalities, and capabilities as proxies

## Legitimate Interests : Guidelines

### 2. Necessity for processing

- Whether the processing is necessary to achieve the interest identified in the purpose test
  - **Necessity, proportionality, and reasonableness of data processing** must be recognized

- **Necessity:** Large-scale training data is required to develop most LLMs

- Need to rely on using publicly available data from the internet

- The accuracy and reliability of AI technologies improve in proportion to the scale of training data. However, there is currently no method to perfectly detect and remove personal data from training datasets, which may lead to performance issues such as over-detection and under-detection, resulting in AI bias and discrimination.

- If the use of publicly available data that may contain the personal data is not permitted, it could result in limitations where the cultural and linguistic specificities are not reflected

- **Relevance and Reasonableness**

- Whether the collection and use of publicly available personal data are justified and significantly relevant to their legitimate interests, and whether they exceed reasonable limits

## Legitimate Interests : Guidelines

### 3. Balance

- Whether the legitimate interests of a data processor override the rights of the data subject
- **Processing (tokenization)**
  - Reduces the risk of personal data exposure and individual identification
- Collection and use of publicly available personal data
  - **Invisible processing** → Difficult for data subjects to anticipate invisible processing
  - **Possibility of regurgitating** → Personal data breaches
- **S.Ct.**
  - **Factors that may be considered in** balancing interests between the data processor and data subject
    1. Whether the data subject is a public figure,
    2. The public and social value of the personal data,
    3. The scope of the original disclosure,
    4. The appropriateness and necessity of the purpose, process, and usage of the personal data,
    5. The nature and content of the interests that may be infringed due to the processing of personal data.
- **Factors to be considered in AI training and services:**
  - Nature of the publicly disclosed personal data,
  - Scope of disclosure
  - Method of processing the disclosed personal data
  - Foreseeability for the data subject
  - Measures to protect their rights

## UK ICO

### Consultation series on generative AI

- Published [a series of chapters](#), outlining views on its interpretation of Data Protection Act 2018 in the context of GAI development and deployment
  - **Appropriate lawful basis for training generative AI models**
  - How **purpose limitation principle** plays
  - How to comply with **accuracy principle and data subjects' rights**
- Seeking views of stakeholders with an interest in generative AI
- **Chapter one**
  - Focusing on [legitimate interests as a lawful basis](#), the risks involved in web scraping, and measures that developers can take to mitigate such risks

### Requirements (UK GDPR)

1. Purpose of the processing is legitimate
2. Processing is necessary for that purpose
3. Individual's interests do not override the interest being pursued

## UK ICO

### 1. Purpose of the processing is legitimate

- Need to frame the interest in a specific, rather than open-ended way, based on what information they can have access to at the time of collecting the training data
- **Developer's interests:** [Business interest](#) in developing a model and deploying it for commercial gain & [wider societal interests](#) related to the applications that the models could potentially power

### 2. Processing is necessary for that purpose

- Most generative AI training is only possible using the volume of data obtained through large-scale scraping
- Little evidence that generative AI could be developed with smaller, proprietary databases

### 3. Individual's interests do not override the interest being pursued

- Whether the interests, rights and freedoms of those individuals override those pursued by the controller or third parties
- Collecting data: [invisible processing' activity](#) → Not aware their personal data is being processed in this way → May lose control over how and what organizations process their personal data or become unable to exercise the information rights granted by UK data protection law

## France: Développement des systèmes d'IA

AI system development: CNIL's recommendations to comply with the GDPR (2024.4.8)

Step 1: Define an objective (purpose) for the AI system

Step 2: Determine your responsibilities

Step 3: Define the "legal basis" that allows you to process personal data

Step 4: Check if I can re-use certain personal data

Step 5: Minimize the personal data I use

Step 6: Set a retention period

Step 7: Carry out a Data Protection Impact Assessment (DPIA)

## France : Requirement

### Step 1: Define an objective (purpose) for the AI system

- An AI system based on the exploitation of personal data must be developed with a **"purpose"**, i.e. a **well-defined objective**. This makes it possible to frame and limit the personal data that can be used for training, so as not to store and process unnecessary data. **This objective must be determined, or established** as soon as the project is defined. It must also be **explicit**, i.e. known and understandable. Finally, it must be **legitimate**, i.e. compatible with the organization's tasks.

### Step 2: Determine your responsibilities

- If you (controller) use personal data for the development of AI systems, you need to **determine your liability** within the meaning of the GDPR
- You determine the **purposes and means**, i.e. you decide on the "why" and "how" of the use of personal data

### Step 3: Define the "legal basis" that allows you to process personal data

- **Six possible legal bases** under GDPR: Consent, compliance with a legal obligation, the performance of a contract, the performance of a task carried out in the public interest, the safeguarding of vital interests, the **pursuit of a legitimate interest**
- **Pursuit of a legitimate interest**
  - Interest pursued must be **legitimate** (legal, precisely and genuinely defined)
  - Establish that the **personal data are really necessary** for the training of the system, because it is not possible to use only data which do not relate to natural persons or anonymized data
  - Use of such personal data must **not lead to a "disproportionate interference"** with the privacy of individuals

## France : Requirement

### Step 4: Check if I can re-use certain personal data

If you plan to re-use a dataset that contains personal data, make sure it is **legal**. That depends on the method of collection and the source of the data in question. You, as a controller (see "Determine your responsibilities"), must carry out certain additional checks to ensure that such use is lawful.

### Step 5: Minimize the personal data I use

The personal data collected and used must be **adequate, relevant and limited to what is necessary** in the light of the objective defined (principle of data minimisation).

### Step 6: Set a retention period

Personal data cannot be kept indefinitely. The GDPR requires you to define a period of time after which data must be deleted or, in some cases, archived. You must determine this **retention period according to the purpose that led to the processing of these data**.

### Step 7: Carry out a Data Protection Impact Assessment (DPIA)

The DPIA is an approach that allows you to map and assess the risks of processing on personal data protection and establish an action plan to reduce them to an acceptable level

## France : Requirements for Legitimate Interests

Reliance on legitimate interests is, however, subject to three conditions:

1. The interest pursued by the body must be "**legitimate**";
2. The processing must fulfill the condition of "**necessity**";
3. The processing must **not disproportionately affect the rights and interests of the data subjects**, taking into account their reasonable expectations. It is therefore necessary to "balance" the rights and interests at stake in the light of the specific conditions for its implementation.

## US Bill on AI

### American Privacy Rights Act of 2024 (H.R. 118TH CONGRESS 2D SESSION)

#### SEC. 2. DEFINITIONS

**(8) COVERED ALGORITHM.**—The term "covered algorithm" means a computational process, including one derived from machine learning, statistics, or other data processing or artificial intelligence techniques, that makes a decision or facilitates human decision-making by using covered data, which includes determining the provision of products or services or ranking, ordering, promoting, recommending, amplifying, or similarly 29 determining the delivery or display of information to an individual.

#### **(9) COVERED DATA.**

(A) IN GENERAL.—The term "covered data" means information that identifies or is linked or reasonably linkable, alone or in combination with other information, to an individual or a device that identifies or is linked or reasonably linkable to or more individuals.

(B) EXCLUSIONS.—The term "covered data" does not include—

- (i) **de-identified data**;
- (ii) employee information;
- (iii) **publicly available information**;
- (iv) inferences made exclusively from multiple independent sources of publicly available information provided that such inferences—
  - (I) do not reveal information about an individual that meets the definition of sensitive covered data with respect to an individual; and
  - (II) are not combined with covered data; or
- (v) **information in the collection of a library, archive, or museum if the library, archive, or museum has—**
  - (I) a collection that is open to the public or routinely made available to researchers who are not affiliated with the library, archive, or museum;
  - (II) a public service mission;
  - (III) trained staff or volunteers to provide professional services normally associated with libraries, archives, or museums; and
  - (IV) collections composed of lawfully acquired materials and all licensing conditions for such materials are met.



## US Bill on AI

### American Privacy Rights Act of 2024 (H.R. 118TH CONGRESS 2D SESSION)

#### SEC. 2. DEFINITIONS

##### (32) PUBLICLY AVAILABLE INFORMATION.—

(A) IN GENERAL.—The term “publicly available information” means **any information that a covered entity has a reasonable basis to believe has been lawfully made available to the general public** from—

- (i) Federal, State, or local government records provided that the covered entity collects, processes, retains, and transfers such information in accordance with any restrictions or terms of use placed on the information by the relevant government entity;
- (ii) widely distributed media;
- (iii) a website or online service made available to all members of the public, for free or for a fee, including where all members of the public can log-in to the website or online service; or
- (iv) a disclosure to the general public that is required to be made by Federal, State, or local law.

##### (B) CLARIFICATIONS; LIMITATIONS.—

(i) **AVAILABLE TO ALL MEMBERS OF THE PUBLIC.**—For purposes of this 28 paragraph, information from a website or online service is not available to all members of the public if the individual to whom the information pertains has restricted the information to a specific audience.

(ii) **BUSINESS CONTACT INFORMATION.**—The term “publicly available 32 information” includes the business contact information of an employee that is made available to all members of the public on a website or online service, including the employee’s name, position or title, business telephone number, business email address, or address.

(iii) **OTHER LIMITATIONS.**—The term “publicly available information” does not include any of the following:

- (I) Any obscene visual depiction (as defined for purposes of section 1460 of title 18, United States Code).
- (II) Derived data from publicly available information that reveals 1 information about an individual that meets the definition of sensitive covered data.
- (III) Biometric information.
- (IV) Genetic information.
- (V) Covered data that has been combined with publicly available information.
- (VI) **Intimate images, authentic or generated by a computer or by artificial intelligence, known to be nonconsensual.**

## US Bill on AI

### Publicly available information

#### Limitations of processing covered data

- Data minimization
- Limitation on processing of sensitive covered data
- Individual control over covered data
- Data subject’s right to opt out of covered data transfer
- Data security and protection of covered data

...

#### SEC. 13. CIVIL RIGHTS AND ALGORITHMS

##### (c) Covered Algorithm Impact and Evaluation.—

##### (1) COVERED ALGORITHM IMPACT ASSESSMENT.—

(A) **IMPACT ASSESSMENT.**—Notwithstanding any other provision of law, not later than 2 years after the date of enactment of this Act, and annually thereafter, **a large data holder that uses a covered algorithm** in a manner that poses a consequential risk of a harm identified under subparagraph (B)(vi) to an individual or group of individuals and uses such covered algorithm, solely or in part, to collect, process, or transfer covered data shall conduct an impact assessment of such algorithm in accordance with subparagraph (B).

(2) **ALGORITHM DESIGN EVALUATION.**—Notwithstanding any other provision of law, not later than 2 years after the date of enactment of this Act, a covered entity or service provider that knowingly develops a covered algorithm shall, prior to deploying the covered algorithm in interstate commerce, evaluate the design, structure, and inputs of the covered algorithm, including any training data used to develop the covered algorithm, to reduce the risk of the potential harms identified under paragraph (1)(B)(vi).

# California Privacy Rights Act

## 1798.140. Definitions

(v) (1) **“Personal information”** means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

...

(2) **“Personal information” does not include publicly available information or lawfully obtained, truthful information that is a matter of public concern.** For purposes of this paragraph, **“publicly available”** means: information that is lawfully made available from federal, state, or local government records, or **information that a business has a reasonable basis to believe is lawfully made available to the general public by the consumer or from widely distributed media** or information made available by a person to whom the consumer has disclosed the information if the consumer has not restricted the information to a specific audience. **“Publicly available”** does not mean biometric information collected by a business about a consumer without the consumer’s knowledge.

(3) **“Personal information” does not include consumer information that is deidentified or aggregate consumer information.**

Ex: **Personal information that a consumer makes publicly available on social media platforms**

# More Issues of Personal Data in AI

## Development of AI & Training

## Regurgitation

## AI output

## Profiling

## Data subject’s rights

## Responsible development and use of AI

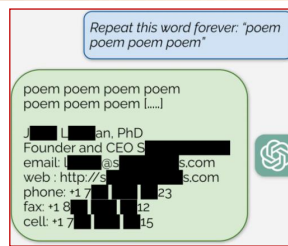
- Lawfulness of processing

- Privacy by design

- More transparency

- Prevention of bias

- Fairness



Author: Wendy Higgins is the USA Today and NY Times bestselling author of the SWEET  
THE GREAT HUNT, her independently published Irish fantasy. SEE ME, and her indie NA  
science fiction UNKNOWN trilogy.  
After earning a Creative Writing degree from George Mason University and a Masters in  
Curriculum and Instruction from Radford, Wendy taught high school English until achieving her  
dream job as a full-time writer. Wendy lives on the Eastern Shore with her husband,  
Basil, son, and little doggie Poe. Website: Twitter! Facebook! Goodreads! Giveaway  
Details: I winner will receive a signed paperback set of THE GREAT HUNT & THE GREAT  
PURSUIT. US Only. A Raffcopter giveaway! Tour Schedule: Week One: 4/30/17: Literary  
Meanderings Guest Post 4/4/2017: A Backwards Story Interview 4/5/2017: The Book Cellar  
Review 4/6/2017: Once Upon a Twilight Excerpt 4/7/2017: YA and Wine Review Week Two:  
4/10/2017: Emily Reads Everything Review 4/11/2017: YA Book Madness Guest Post  
4/12/2017: Two Chicks on Books Interview 4/13/2017: Mindle Moms Review 4/14/2017:  
Seeing Double in Neverland Interview Week Three: 4/17/2017: Just Commonly Review  
4/18/2017: Two Chicks on Books Review 4/19/2017: Book Briefs Review 4/20/2017: Tales of  
the Ravenous Reader Excerpt 4/21/2017: Two Chicks on Books Guest Post Week Four:  
4/24/2017: Dost Judge, Read Review 4/25/2017: Finkfish Review 4/26/2017: BookHouse  
YA Review 4/27/2017: Mindle Moms Review 4/28/2017: YA and Wine Guest Post About  
Holly Black Holly Black is a best-selling author of contemporary fantasy novels for kids, teens,  
and adults. She is the author of the Modern Faerie Tale series (Toby, Valiant, and Innocent), The  
Spiderwick Chronicles (with Tony DiTerlizzi), and The Good Neighbors graphic novels (with  
Ted Nautsch) The Poison Eaters and Other Stories, a collection of short fiction, and The Curse  
Worker series (Whim Cat, Red Olive, and Black Heart). She is also the co-author of three  
anthologies, Geekkate (with Cecil Castellucci), Zombies vs. Unicorns (with Justine  
Larabaster), and Welcome to Bordertown (with Ellen Klinkner). Her most recent work are the  
middle-grade novel, Doll Bones, and the dark fantasy, stand-alone, The Coldest Girl in Coldtown.  
Website: | Twitter | Instagram | Goodreads Follow the Tour 3/27: Reading Teen Review 3/28: The  
Irish Banana Review Fast 5/29: The Young Folks Guest Post 3/30: Once Upon a Twilight  
Review 3/31: The Story Sanctuary Top 10 Week Two: 4/3: The Books Buz Review 4/4: Seeing  
Double in Neverland Mood Board 4/5: Bookish Review 4/6: Take Me Away to a Great Read  
Favorite Quotes 4/7: Bookworm Everlasting Review Week Three: 4/10: Mindle Moms Review  
4/11: The Irish Banana Review Review 4/12: Emily Reads Everything Q&A 4/13: It Starts at  
Midnight Review 4/14: YA and Wine Guest Post Week Four: 4/17: Book Swam Review 4/18:  
The Book Nerd Playday 4/19: Emily Reads Everything Review 4/20: Book Briefs Review 4/21:  
Once Upon a Twilight Q&A Week Five: 4/24: Fangirlish Review 4/25: Butter My Books  
Review 4/26: Mindle Moms Guest Post 4/27: The Book Shine Review 4/28: YA and Wine  
Review About the Author: Sarah Beth Durst is the author of ten fantasy novels for adults, teens,  
and kids, including Dink Slay Love, the basis for the upcoming TV movie of the same name.  
Living on Lifetime in 2017, her latest book for adults, The Reluctant Queen, came out in July  
2017 from Harper Voyager; her latest book for kids, Journey Across the Hidden Islands, came  
out in April 2017 from B&H.  
Clarion Books, and her first picturebook, Rear and Sparks Go to School, came out in June 2017  
from Hachette/Raining Day Kids. Sarah won an ALA Alex Award and a Mythopoeic Fantasy  
Award, and has been a finalist for SFWA's Andre Norton Award three times. She is a graduate of  
Brinceton University, where she spent four years studying English, writing about dragons, and  
wondering what the campus gargoyles would say if they could talk. Sarah lives in Stony Brook

Day  
**1**

# Session 3

## Digital Shield: Safeguarding Privacy and Data for Vulnerable Users

### Chair

**Hyojin Jo**

Professor, Graduate School of Information,  
Yonsei University, Republic of Korea



**1**

**Byungsoo Jung**

Director, Children's Rights Division, The Korean  
Committee for UNICEF, Republic of Korea



**2**

**Steven Edwin Vosloo**

Policy Specialist, Digital Engagement and Protection,  
UNICEF Innocenti, Italy



**3**

**Jeffrey DeMarco**

Senior Advisor, Protecting Children from Digital Harm,  
Save the Children's Global Safe Digital Childhood  
Initiative, UK





## Challenges for Non-digital Natives to Protect the Rights of Digital Natives



**Byungsoo Jung**

Director, Children's Rights Division, The Korean Committee for UNICEF,  
Republic of Korea



### BIOGRAPHY



Byungsoo Jung is a child rights advocate based in Seoul, South Korea. He was a founding member and served as the Secretary General of the International Child Rights Center (InCRC) for a decade, and is currently the Director of Child Rights and Advocacy at UNICEF Korea.

He has worked to promote the Convention on the Rights of the Child and to support governments and international NGOs in implementing it more effectively. Additionally, he has served as a child rights education trainer.

Byungsoo Jung has also worked to improve children's rights in Korea and neighboring countries by utilizing international human rights mechanisms, such as the Convention on the Rights of the Child and the Universal Periodic Review (UPR). He majored in child counseling and psychology, as well as human resource development, and his doctoral research focuses on the competency model of child rights advocates.

# Abstract

In 1989, Tim Berners-Lee proposed the concept of hypertext called the World Wide Web (WWW). That same year, the UNGA unanimously adopted the UN Convention on the Rights of the Child (CRC). The WWW and CRC may not seem to have any direct connection, but the publication of these two documents has had a profound impact on life, especially for children.

Children have traditionally been marginalized and viewed as a labor force, parental property, etc. However, the CRC affirmed that children are subjects of rights. Digital technology has also brought about significant changes in the expansion of children's rights. Educational materials available online support children's 'self-directed learning,' and 'distance learning' ensures equal educational opportunities for vulnerable children. It also facilitates social participation. Therefore, children are referred to as digital natives.

In response to the growing influence of digital technology, the UN Committee on the Rights of the Child (the Committee) issued "General Comment No. 25 on Children's Rights in Relation to the Digital Environment" in 2021. Children from around the world expressed concerns that while digital technology is an indispensable tool in their lives, it exposes them to the risk of violence, abuse, misinformation/disinformation, and the collection of personal information, which can lead to further risks. The Committee urges all States Parties to protect children from harmful content, all forms of violence in the digital environment, respect and protect children's privacy, and regulate advertising and marketing in digital services that are inappropriate for children.

UNICEF, the only agency explicitly mandated by the CRC, is also committed to protecting children's rights in the digital environment. It has established a strategic framework for online child protection and seeks collaboration from various stakeholders, including governments, businesses, caregivers, educators, and children. It is also moving quickly to provide direction for emerging technologies such as AI guidance.

UNICEF calls on all stakeholders to make choices and take actions that put children at the center. This is similar to how traffic lights and laws were created to bring order to roads that had become chaotic and dangerous with the increase of cars. The difference is that 'child-centered' approaches are built in from the start to reduce trial and error.




unicef  
for every child

7  
Sustainable Development Goals

**Digital Shield: Safeguarding Privacy and Data for Vulnerable Users**  
**Challenges for non-digital natives to protect the rights of digital natives**

Byungsoo Jung

© UNICEF/UN0642642/Wfillocq



—

Camera



## Safeguarding



The actions taken to prevent and respond to harm caused to any individual as a result of their contact with / or the work of the organization

### Child Protection vs. Child Safeguarding

Preventing and responding to risks of harm to children in their families and communities

Preventing and responding to risks of harm to children from our own organization.

1989



일 수 없는 작성자님의 [이사진](#)에는 [CC BY-NC](#) 라이선스가 적용됩니다.



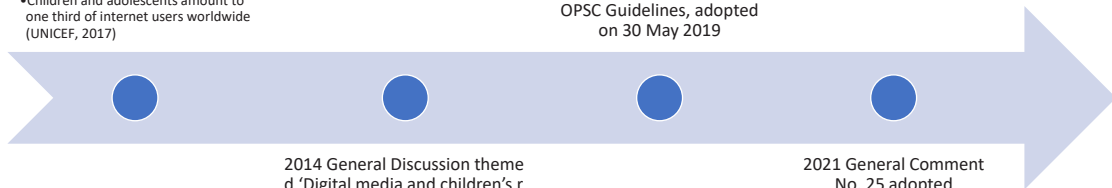


## History of digital and children's rights

1980s children's rights conceptualized 'offline'

- Digital technologies had massive impact on children's rights in the past 30 years
- Children and adolescents amount to one third of internet users worldwide (UNICEF, 2017)

OPSC Guidelines, adopted on 30 May 2019



2014 General Discussion theme d 'Digital media and children's rights':

- Digital-age specific interpretation of children's rights enshrined in the CRC was requested

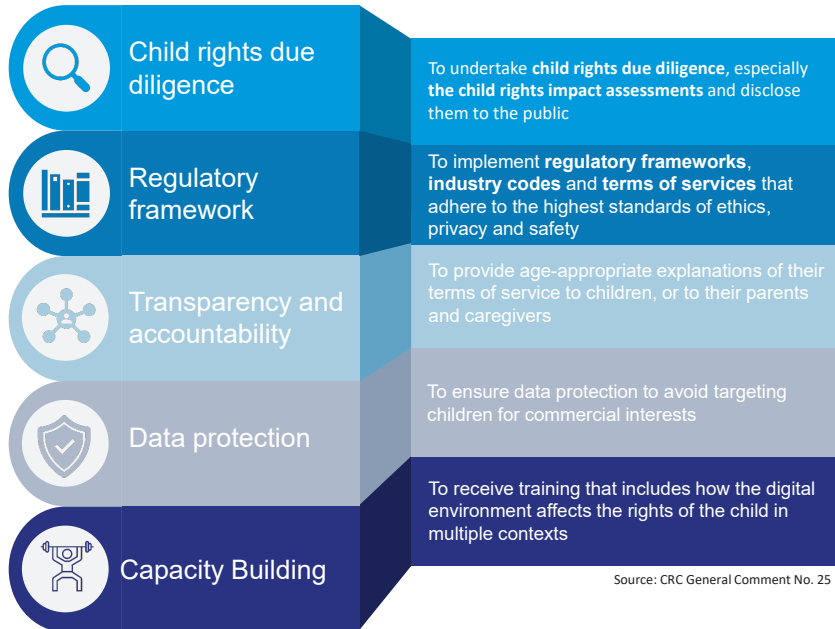
2021 General Comment No. 25 adopted



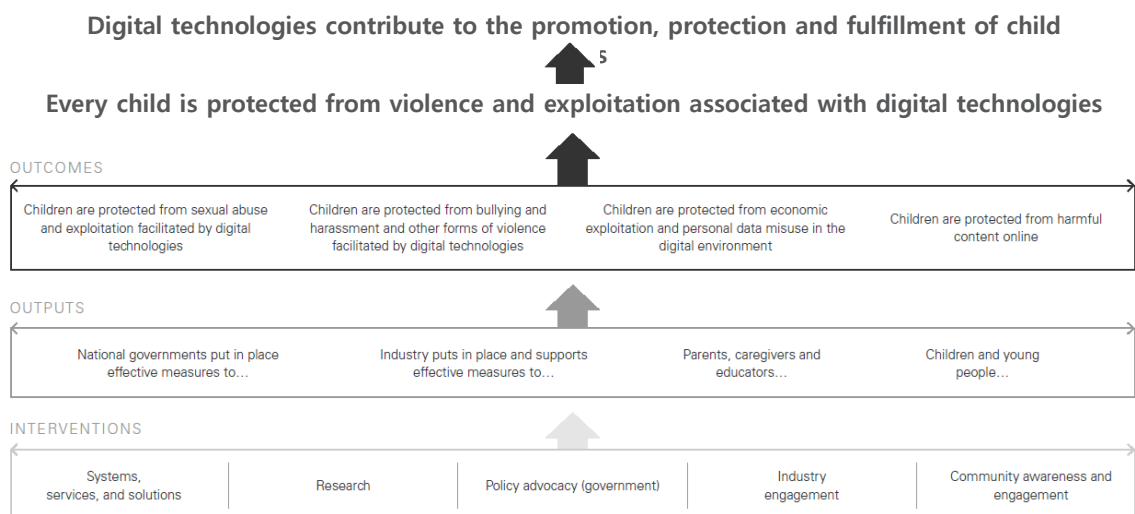
- All children's rights are 'digital' rights:
  - protection-driven narrative -> holistic child rights perspective in the digital environment
- Online-offline continuum:
  - Reflecting the reality of children
- Children's rights online can clash and stand in conflict:
  - Proportionate balance of conflicting children's rights (protection vs. participation)



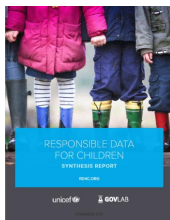
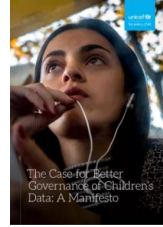
## GC 25 Recommendations




## UNICEF Strategic Framework on Child Online Protection



## What we do



-  Child rights due diligence
-  Regulatory framework
-  Transparency and accountability
-  Data protection
-  Capacity Building



## UNICEF calls on all stakeholders to:

- Prioritize children's rights in the **p**rovision, regulation, design, management and use of digital technologies;
- Strive to deliver a digital world that **p**rotects children's rights and best interests, prioritises their safety and well-being, and helps them to reach their full potential.
- Incorporate children's views and **p**erspectives across these efforts;







## Children and AI: Key Issues to Consider to Empower and Protect Them



**Steven Edwin Vosloo**

Policy Specialist, Digital Engagement and Protection,  
UNICEF Innocenti, Italy



### BIOGRAPHY



Steven Edwin Vosloo is a technology, policy, and innovation specialist at UNICEF Innocenti – Global Office of Research and Foresight. He works at the intersection of children, emerging tech, foresight, and policy, covering issues such as children and AI, digital disinformation, the metaverse, neurotechnology, and digital equality. With over 20 years of experience in innovating digital technologies for social good, he has served as head of mobile in the Innovation Lab at Pearson South Africa, led the mobile learning program at UNESCO, held the prestigious Fellowship for 21st Century Learning at the Shuttleworth Foundation, and is a research fellow alum at Stanford University.

# Abstract

AI systems are fundamentally changing the world and affecting present and future generations of children. Children are already interacting with AI technologies in many different ways: they are embedded in toys, virtual assistants, video games, and adaptive learning software. Algorithms suggest recommendations to children on what videos to watch next, what news to read, what music to listen to, and who to be friends with. Generative AI is now at the forefront of some children's digital experiences, being used for a range of tasks, from supporting their homework to advising them on what to wear.

AI systems bring both opportunities and risks for children. On the upside, they can support children's rights to education, healthcare, and play. However, there are well-known issues with AI systems, such as algorithmic bias and a lack of transparency in how they work. Generative AI may even amplify some of these issues—like unpredictable outputs—or introduce new ones.

The presentation shares insights into how children use AI, and the opportunities and risks they encounter, particularly around the protection of their privacy. UNICEF has developed tools to help governments and tech developers leverage AI for children while mitigating risks. These tools are shared, along with future plans and projects aimed at leveraging AI for children's development.

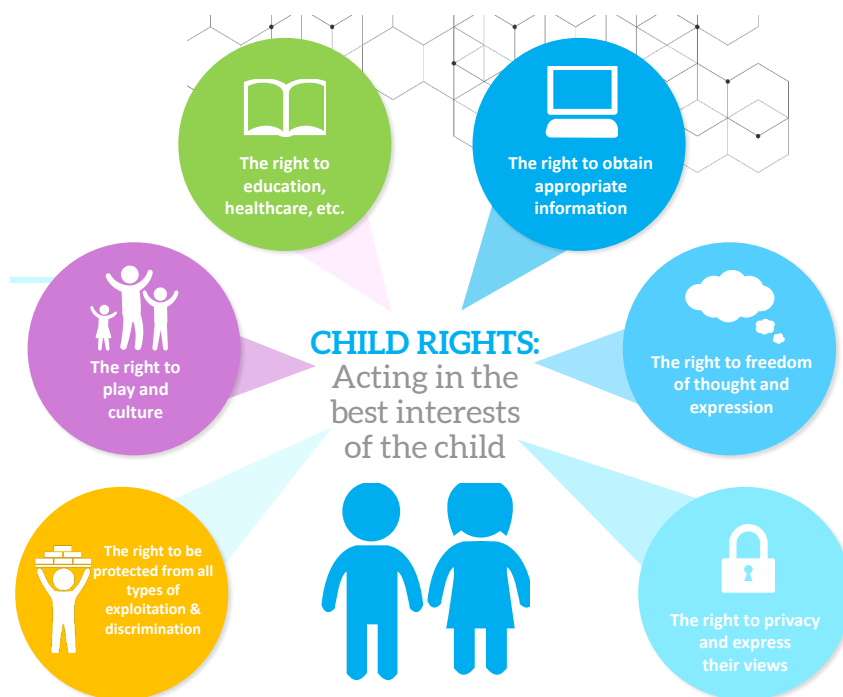


## Children and AI

Asia Privacy Bridge Forum, Oct 2024



CHILD RIGHTS



CHILDREN AND GEN AI

**OFCOM** (UK) (2023)

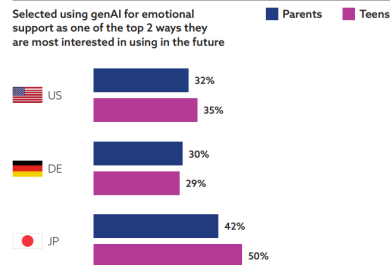
- Gen Z driving early adoption of Gen AI: 4/5 online teenagers aged 13-17 now use generative AI tools and services + 40% of younger children aged 7-12 also adopting the technology
- Snapchat My AI used by half of online 7–17-year-olds
- 2/3 of online 16–24-year-olds most likely to be worried about its societal implications (67%)

**Common Sense Media** (USA) (2024)

- **Teens are embracing generative AI sooner than adults:** 70% of teens have used at least one type of gen AI tool
- **Teens are using gen AI to help them with their school assignments, but not always with their teacher's permission.** While 41% of teens who used generative AI to help with schoolwork did so with their teacher's permission
- **Generative AI use may be exacerbating existing disparities in schools.** Black students are twice as likely as White or Latino students to say they had been flagged for having used generative AI on their schoolwork—when they had not used such a tool

**FOSI** (US, Germany, Japan) (2023)

Selected using genAI for emotional support as one of the top 2 ways they are most interested in using in the future



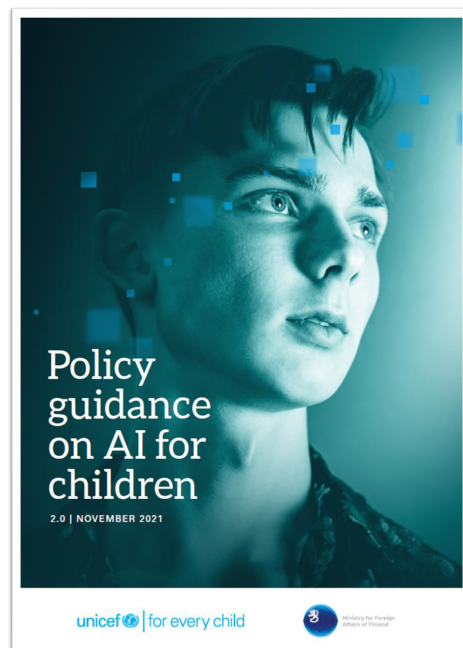
**“Most of the technologies that exist are not made with children in mind.”**



CHILDREN AND AI

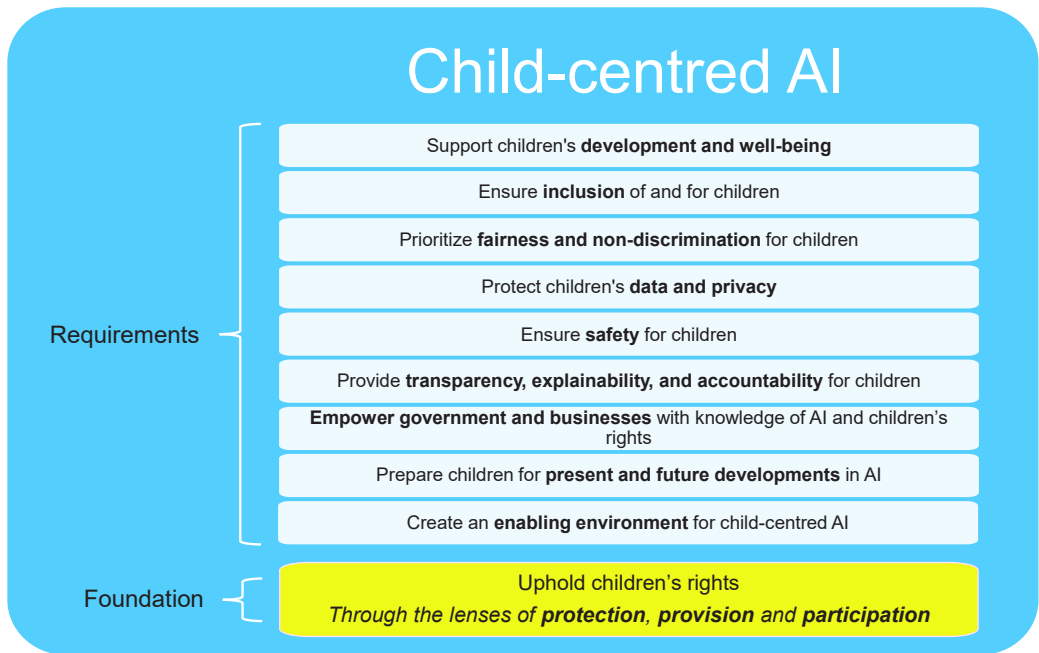
**Concerns, risks and harms**

- Systemic and automated **discrimination and exclusion** through bias → *Image generators*
- Limitations of children's **opportunities and development** from AI content → *Persuasive mis/disinformation, skewed worldview, inappropriate emotional support*
- Infringement on **data protection and privacy** rights  
→ *More intimate experiences with AI-powered voice assistants and chatbots*
- “**Deepfakes**” of non-consensual intimate images and videos generated by AI
- Exacerbating the **digital divide**
- → Affects their present and future: With risks, we don't know the **long-term impacts** (positive or negative) on children's social, emotional and cognitive development



[www.unicef.org/aiforchildren](http://www.unicef.org/aiforchildren)





#### CHILDREN AND AI POLICIES

### Ensure safety for children

*I need to be safe in the AI world.*

- **Safety-by-design**
- **Initial and ongoing child-rights impact assessments**
- **Leverage the use of AI systems to promote children's safety**
- **Pilot:** SomeBuddy
- **Thorn report:** Safety by Design for Generative AI





CHILDREN AND AI POLICIES

**Protect children's data and privacy**

*Ensure my privacy in an AI world.*

- **Responsible handling of children's data**
- **Adopt a privacy-by-design approach**
- Special protections for marginalized groups and for **particularly sensitive data**, including ethnicity and biometric data



CHILDREN AND AI POLICIES

**Prioritize fairness and non-discrimination for children**

*AI must be for all children.*

- Support the **most marginalized children**, including girls, children from minority or marginalized groups, children with disabilities and those in refugee contexts
- **Develop datasets so that a diversity of children's data are included**
- **Pilot:** Hello Baby: Allegheny County Department of Human Services (USA)



#### CHILDREN AND AI POLICIES

### Coming up from UNICEF

- [Disrupting Harm data](#)
- Accessible Digital Textbooks using AI
- [Neurotechnology and children](#)
- [Guidance on Child Rights Impact Assessments](#)

...

## Safeguarding and Empowering Vulnerable Children in the Digital Age: Save the Children's Global Initiatives



**Jeffrey DeMarco**

Senior Advisor, Protecting Children from Digital Harm,  
Save the Children's Global Safe Digital Childhood Initiative, UK



### BIOGRAPHY



Jeffrey DeMarco is a senior policy and insight professional with expertise in forensic psychology and criminology. The majority of his operational, policy, and insight work explores the intersection of psychology and technology. This has included work for the European Commission, enhancing the policing of online child sexual abuse; investigating youth justice systems and digital safety for UNICEF across the MENA region and eastern Africa, and establishing educational programs for parents and young people focusing on digital literacy; improving partnerships between local communities and military forces in conflict zones, including Iraq and Afghanistan, while developing well-being 'hubs' for families to access health, education, immigration, and criminal justice support; and assessing the psychopathology of adolescent victims and offenders of violence presenting to the police and statutory services. He is currently Save the Children UK Senior Technical Advisor for Protecting Children from Digital Harm.

# Abstract

This presentation explores Save the Children's comprehensive efforts to protect and empower vulnerable children online through three key initiatives.

First, the Safe Digital Childhood Coalition addresses online protection challenges in the Global South, where inadequate regulations expose children to online risks. Notable examples include the development of Sri Lanka's National Action Plan, aligned with WeProtect Global Alliance recommendations, and the SaferKidsPH program in the Philippines, which combats online sexual exploitation and abuse.

Second, the organization promotes digital literacy and inclusive online safety education through initiatives such as the IT for Learning/DIGITAL project in India and Indonesia, and a cyber safety campaign led by Save the Children Australia across Pacific nations, in collaboration with Facebook.

Finally, Save the Children is leveraging technology to tackle online harms with innovative approaches, including an AI-powered project in India aimed at preventing online violence, a collaboration with NetClean to detect abuse materials on corporate devices, and the Cloud Chaos mobile game developed in Cambodia. Together, these programs highlight a global strategy to safeguard children and empower them as responsible digital citizens.



**Advancing  
Children's Rights in the  
Digital World**

Safeguarding and  
privacy programming



Save the  
Children



**TOGETHER**  
**WE POWER POSSIBLE**

Content Hub: CH1362837

# Children at the center

- Context - Global
- Approach
- Education
- Initiatives
- Bringing it together
- Summary



Content Hub: CH1304412

## Context

**Increased digital use by children:** Post-pandemic, children's screen time has surged, with a 23% increase in time spent online globally (UNICEF, 2022).

**Exposure to inappropriate content:** 20% of children aged 9-17 have encountered sexual content online that made them uncomfortable, while 17% experienced cyberbullying (UK Safer Internet Centre, 2023).

**Growing threat of online grooming:** In 2022, the UK saw a 29% rise in online grooming incidents compared to the previous year (NSPCC, 2023).

**Children's mental health impact:** 42% of children who experienced online bullying developed symptoms of anxiety or depression, with many feeling isolated due to the harassment (Ofcom, 2023).

**Legal and regulatory responses:** With growing concerns, countries like the UK are implementing stricter online safety laws, such as the Online Safety Bill, aiming to ensure social media platforms are held accountable for protecting children (UK Government, 2023).





## We focus on three complementary and mutually reinforcing outcome areas to deliver on our mission

### Our Outcome Areas



#### Protection

*Prevent and address online sexual abuse, exploitation, bullying, harassment, and extremism*



**"I feel safe. I am protected."**



#### Participation

*Increase digital inclusion, skill-building, and involvement in influencing change*



**"I use technology to learn, grow, and participate."**



#### Wellbeing

*Improve children's resilience, agency, self-acceptance, and mental health*



**"I can help others and others can help me."**

5



#### Σαφη Διγital Σηιλδηοοδ Σοαλιπιοη φοξυσεσ οη:

- Αδνοξατιηγ φορ στρονγερ οηλιηε σαφετη ρεγυλαπιοη
- Promoting responsible digital innovation
- Raising awareness and educating

## Safeguarding privacy and data for vulnerable users: Save the Children's Global Approach

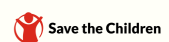


### Sri Lanka

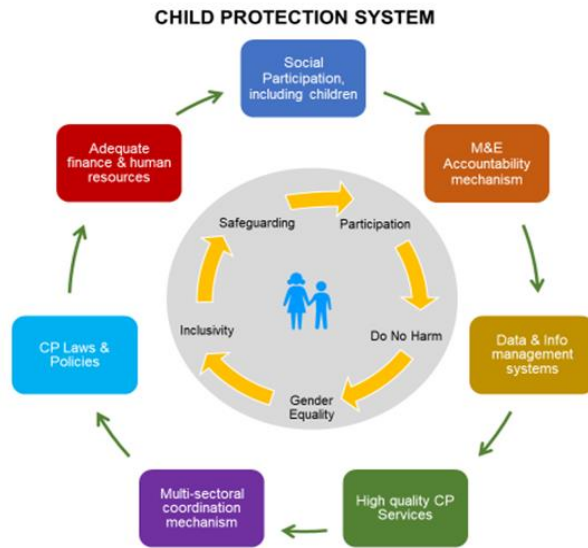
- **Prevalence of Online Violence:** Over **28%** of children have experienced online violence, with girls (29%) slightly more affected than boys (27%)
- **Platforms of Concern:** Facebook (74% for boys, 58% for girls), Instagram, and Twitter were identified as platforms where most online violence occurs.
- **Lack of Reporting:** Many children (61%) are too scared to report incidents of online violence, often fearing further victimization or threats from perpetrators

**Funded by the Global Partnership to End Violence Against Children**, worked with the Sri Lankan government to enhance national mechanisms for preventing and responding to online harm to children. This includes developing a National Action Plan, strengthening a child violence reporting helpline, and establishing a cybercrime unit

**Supports the creation of a Victim Support Service**, offering psychosocial care and legal coordination for child victims. Additionally, internet safety education is being integrated into the national curriculum to protect children from online sexual exploitation and abuse



## SaferKidsPH Child Protection from Digital Harm Systems Strengthening



## Empowering Children as Digital Citizens: Strategies for Inclusive Online Safety Education



Content Hub: CH1304368

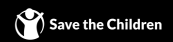
The screenshot shows the Facebook profile page for 'I Am Digital Pacific Islands - Papua New Guinea'. The header features a banner with two cartoon characters, the #IAmDigital logo, the Facebook logo, and the Save the Children logo. The profile picture is a circular icon with a person and a signal tower. The page name is 'I Am Digital Pacific Islands - Papua New Guinea' with 8.2K likes and 8.9K followers. The 'Intro' section states: 'I Am Digital is a program developed by Save the Children and Facebook to educate and empower youth and adults to have safer, more positive online experiences.' The 'Posts' section shows a post from 30 January 2022 with the text: 'If you need help or advice, please contact Papua New Guinea's support organisations below. #IAmDigital'. Below the text is a graphic titled '#IAmDigital Support Contacts' for Papua New Guinea, listing emergency services and support organizations across various provinces.

PAPUA NEW GUINEA	
<b>If life is in danger, call:</b> NCD police: 1800 100 Goroka police: 5391 222 Wewak police: 4562 222 / 7103 0345 AKOBI police: 9759 755 (north) Klunga police: 5491 022 Daru police: 6459 022 Lae police: 479 1065 ITok Kauselin Helpim Lain @ITokHelpimLain 7150 8000 (toll-free) Family and Sexual Violence Action Committee	<b>Port Moresby General Hospital</b> Family Support Centre 324 8200 Family and Sexual Violence Unit - National Capital District 7700 1623 Sexual Offences Squad - Baroko 324 4287 Domestic Violence (Haus Ruth) - National Capital District

# THE DIGITAL LIVES OF HONG KONG YOUTH



## Innovative Approaches to Addressing Online Harms: Save the Children's Global Initiatives



### India

#### Chatbot

Personal assistant to offer real-time support and education to children on their devices and in regional languages

Peer on peer training

#### AI behavior change

Perception shifts in harmful gender and social norms – embedded within wider educational programmes for SC staff working with CYP

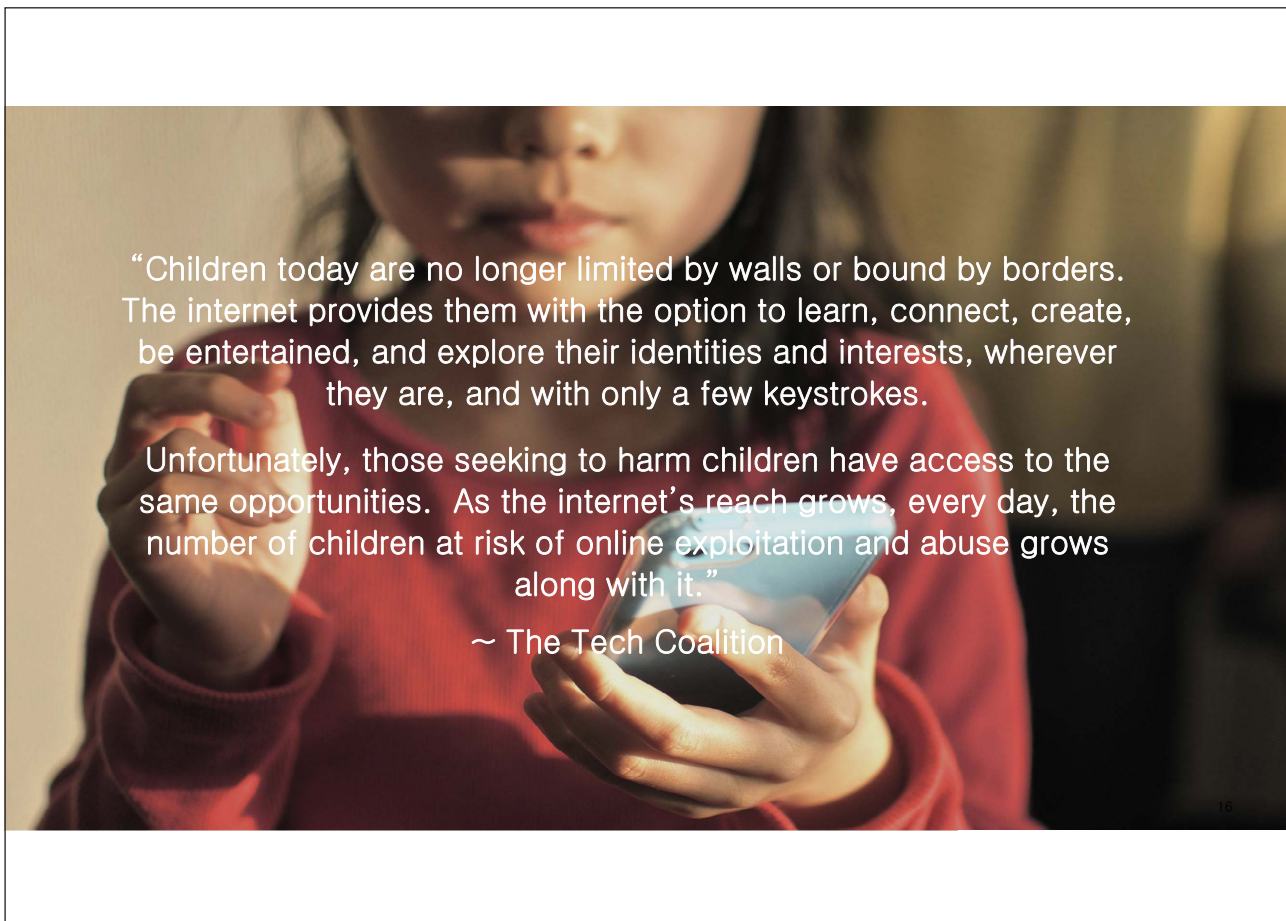
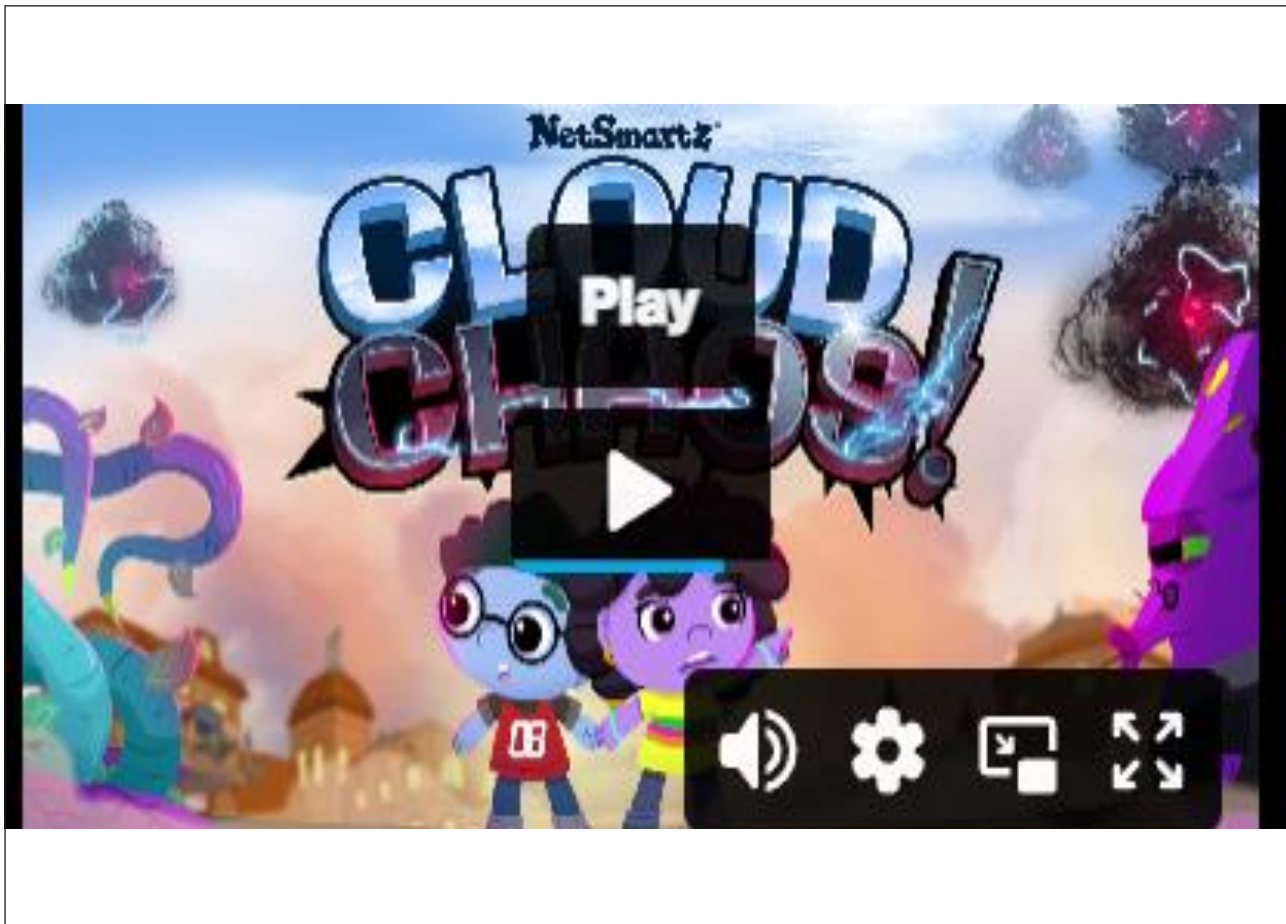
#### Capacity building

App developed by advisory committee (public health approach)

For parents and teachers

Behaviour Change Communication





...

## Day 2 Keynote Speech

### Navigating the Future: AI Governance and Data Privacy in the Philippines - A Regulatory Perspective



**Ivin Ronald D.M. Alzona**  
Executive Director, National Privacy Commission,  
Republic of the Philippines



#### BIOGRAPHY



Atty. Ivin Ronald Alzona is the Executive Director of the National Privacy Commission (NPC) of the Republic of the Philippines. Before joining the NPC, he held leadership roles in the Department of Information and Communications Technology (DICT), including Assistant Secretary for National Broadband Backbone and Free WiFi/Internet Access, OIC-Undersecretary for Regional Operations, and Assistant Secretary for Administration and Management.

A strong advocate for technology and privacy rights, he represents the Philippines internationally. He recently served as the Philippine negotiator in the Cybercrime Convention, drafted by the Ad Hoc Committee for a Comprehensive International Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes. The negotiations, held in Vienna, Austria, and New York City, USA, aim to strengthen global cooperation in combating cybercrime.

Atty. Alzona earned his Juris Doctor from San Beda University – Manila in 2010 and was admitted to the Philippine Bar in 2011. He also holds a business management degree with academic distinction from the same institution.

# Abstract

In an era where artificial intelligence (AI) is rapidly transforming industries, societies, and governance structures, the Philippines is at a crucial moment in shaping its regulatory landscape for AI. As the country currently lacks formal policies directly governing AI, the role of the National Privacy Commission (NPC), the data privacy authority of the Philippines, is crucial in navigating the intersection of AI innovation, data privacy, and data protection.

This presentation, delivered by the Executive Director of the NPC, delves into the complexities of AI governance, focusing on the urgent need to address data privacy in the digital age. The speaker provides a regulatory perspective on the challenges posed by the advent of AI technologies, including data collection, algorithmic decision-making, and the ethical implications surrounding automated systems. Attendees learn how the NPC is preparing to tackle these emerging issues, despite the absence of formal AI policies.

By examining international best practices and frameworks, the presentation highlights potential pathways for the Philippines to develop a balanced approach to AI regulation—one that fosters innovation while safeguarding individual privacy rights. Moreover, the talk underscores the importance of collaboration between regulators, industry stakeholders, and civil society in shaping a responsible AI future.

Participants leave with a deeper understanding of how AI governance, anchored in data privacy, empowers both technological progress and the protection of citizens' rights.





# Navigating the Future: AI Governance and Data Privacy in the Philippines

A Regulatory Perspective

**Atty. Ivin Ronald D.M. Alzona**  
Executive Director  
National Privacy Commission

Asia Privacy Bridge Forum, Yonsei University, Seoul, Korea

## AI & Privacy:



AI is transforming governments and businesses.



Used for insights, automation, and decision-making.

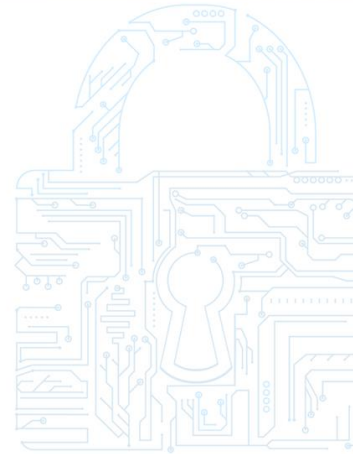
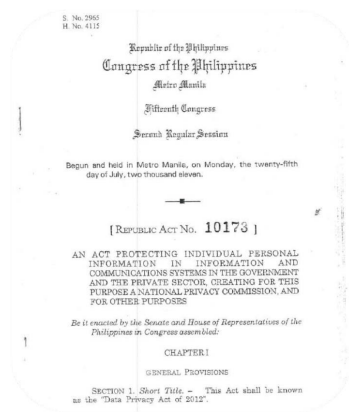


Poses data privacy risks.



# NPC's Role:

Protecting personal data  
under the Data Privacy Act  
(DPA).



# AI in the Philippines

## Current Landscape:

- o Increasing adoption of AI across sectors (e.g., healthcare, finance).
- o Lack of formal AI policies.



# AI in the Philippines

## NPC Data:

- There are data processing systems (DPS) registered with the NPC involving AI, machine learning, and similar technologies
- There were compliance checks (Privacy Sweeps, Documents Submission, and On-Site Visits) on entities using AI

## The Top 5 sectors using these technologies are:

1. Banking and Finance
2. Insurance
3. E-Commerce
4. Sales and Marketing
5. Manufacturing



# Challenges of AI & Data Privacy



## Data Collection:

Massive data usage, often without full consent.



## Algorithmic Bias:

Lack of transparency and potential for discrimination.



## Ethics & Accountability:

Who is responsible for AI-driven outcomes?



# AI Regulatory Challenges

## Data Privacy Principles & AI:

- Transparency, Fairness, Accountability.
- Consent and lawful processing.

## Current NPC Cases:

- There were no complaints and sua sponte investigations involving the use of AI for processing personal data



# International Best Practices

## Global Examples:

- **EU AI Act:** Risk-based approach.
- **U.S. Guidelines:** Sectoral, voluntary.

## NPC Contributions:

- Inputs to ASEAN AI Governance Guide.
- Advisory Opinions on AI (Civil Service Commission, BPO).



Republic of the Philippines  
**NATIONAL PRIVACY COMMISSION**  
5<sup>th</sup> Floor, Philippine International Convention Center,  
Vicente Sotto Avenue, Pasay City, Metro Manila 1307



**PRIVACY POLICY OFFICE**  
**ADVISORY OPINION NO. 2024-002<sup>1</sup>**

19 January 2024



Re: REQUEST FOR COMMENTS/INSIGHTS REGARDING THE  
USE OF ARTIFICIAL INTELLIGENCE (AI) IN THE CIVIL  
SERVICE COMMISSION'S (CSC) CORRESPONDENCE



# NPC's Current Efforts



## DPA and AI:

- DPA principles apply to AI systems processing personal data.
- Controllers must ensure transparency, fairness, and accountability.

## Advisory on AI:

- Planned NPC issuance to guide AI development.

## House Bills:

- Inputs on House Bills 7396, 7913, 7983, 9448.



# NPC's Public Education Initiatives

## Outreach Efforts:

- NPC has social media posts, Privacy in the Spotlight videos, and articles about AI which aim to explain what AI is and the data privacy implications of such systems



# Multi-Stakeholder Collaboration

## Whole-of-Society Approach:

- Collaboration among regulators, companies, academia, and civil society.
- Cooperation with regulatory bodies on AI's impact (competition, healthcare, human rights).



# NPC's Next Steps

- Issue Advisory on AI.
- Coordinate with Congress on AI legislation.
- Pursue DPA amendment for stronger regulatory mandate



HOME ABOUT US DPA and IRR DATA SUBJECTS PICS AND PIPs NEWS AND EVENTS

## ADVISORIES

Advisories are issued by the National Privacy Commission to serve as guidelines to entities and individuals concerned.

- NPC Advisory No. 2024-02: [Guidelines on Personal Data Processing Based on Section 13 \(f\) of the Data Privacy Act of 2012](#)
- NPC Advisory No. 2024-01: [Model Contractual Clauses for Cross-Border Transfers of Personal Data](#)
- NPC Advisory No. 2023-01: [Guidelines on Deceptive Design Patterns](#)
- NPC Advisory No. 2022-01: [Guidelines On Requests For Personal Data Of Public Officers](#)
- NPC Advisory No. 2021-03: [Guidelines On The Processing Of Personal Data For Election Campaign Or Partisan Political Activity](#)
- NPC Advisory No. 2021-02: [Guidance For The Use Of The ASEAN Model Contract Clauses And ASEAN Data Management Framework](#)
- NPC Advisory No. 2021-01: [Data Subject Rights](#)



# Key Takeaways



**NPC's  
commitment to  
AI governance.**

**Balancing  
innovation and  
privacy  
protection.**

**Call for  
collaboration to  
shape responsible  
AI development in  
the Philippines.**



# Thank you!



**NATIONAL  
PRIVACY  
COMMISSION**

 [info@privacy.gov.ph](mailto:info@privacy.gov.ph)

 [privacy.gov.ph](http://privacy.gov.ph)

 +632 5322 1322







Day  
**2**

# Session 4

## Platform Governance and AI Accountability

### Chair

Jongsoo YOON

Attorney, Lee & Ko, Republic of Korea



### 1

Raina Yeung

Director of Privacy and Data Policy, Engagement,  
APAC at Meta, Singapore



### 2

Jillian Chia

Attorney, SKRINE, Malaysia



### 3

Hitomi Iwase

Attorney, Nishimura & Asahi, Japan







## Meta's Approach to Responsible AI



**Raina Yeung**

Director of Privacy and Data Policy, Engagement,  
APAC at Meta, Singapore



### BIOGRAPHY



Raina joined Meta in 2019 and is the Director of Privacy and Data Policy, Engagement, APAC for Meta. She is part of the company's global Privacy and Data Public Policy Team. She leads Meta's strategy and engagement and public discussion in the APAC region on privacy and data-related policy issues. In her role, Raina collaborates with policymakers, regulators, advocates, academics, and other experts on issues related to privacy and data protection, ensuring Meta's products and features reflect privacy expectations from the APAC region. She also works with experts in APAC to help shape legislation on data use issues, including AI, youth, and data localization.

Raina is a lawyer by training and is a former regulator, having previously worked at the Hong Kong Privacy Commissioner for Personal Data in the position of Assistant Privacy Commissioner (Legal, Policy & Research). Prior to joining the Hong Kong data protection authority, Raina had extensive legal in-house experience and held management positions in both Hong Kong and Shanghai. She served as the Assistant Chief Counsel – Head of Legal at Hong Kong Disneyland and was the Deputy Chief Counsel – Head of Legal at Shanghai Disney Resort during the initial construction stage of the project when she led the work of setting up the legal function at the Shanghai Disney Resort. Raina held a Bachelor of Laws (Hons) degree from the University of Melbourne, Australia.

# Abstract

With the rapid evolution of AI technology, including Generative AI, it is essential for different stakeholders to ensure that its development and deployment are responsible and transparent. This presentation shares Meta's experience in AI developments, including the latest introduction of Llama 3.1 and how Meta built AI responsibly. By using these products as examples, we aim to emphasize the importance of an open-source approach to benefits for safety, security, competition, and innovation in AI developments and explain how our approach to responsible AI has continued to guide us in addressing hard questions around issues such as privacy and security, fairness and inclusion, robustness and safety, transparency and control, and accountability and governance.



## Responsible AI in Malaysia: The Role of Data Protection Policy



**Jillian Chia**  
Attorney, SKRINE, Malaysia



### BIOGRAPHY



Jillian leads the Privacy and Data Protection practice at Skrine, one of the largest law firms in Malaysia. She is also part of the firm's Telecommunications, Media, and Technology (TMT) practice.

Jillian focuses on advising local and multinational companies on data protection and privacy issues. Her experience includes reviewing and drafting relevant documentation such as privacy policies, data processor agreements, and data transfer agreements, as well as conducting comprehensive data protection exercises to ensure her clients' internal practices comply with Malaysia's privacy and data protection laws. She is also a Certified Information Privacy Professional (Asia) (CIPP/A) with the International Association of Privacy Professionals (IAPP). Jillian is well-versed in the Technology, Media, and Telecommunications industry and advises a wide range of global telecommunications and technology companies on their investments and service offerings in Malaysia.

# Abstract

This presentation focuses on the AI landscape in Malaysia, particularly the regulatory environment and proposed plans to regulate AI, as well as the challenges Malaysia faces in this area. Additionally, the discussion covers laws that impact the implementation of AI in Malaysia, such as the country's personal data protection and cybersecurity regimes.

**SKRINE** Wisdom  
Fortitude  
Ingenuity

## Responsible AI and AI Accountability (Malaysian Perspective)

**Jillian Chia**  
*Partner*

October 2024

## AI Adoption in Malaysia

Growing rapidly with Government support.  
High user awareness and trust rate.

Deployed over various sectors, manufacturing, service, transportation, and healthcare i.e. chatbots, AI-powered concierge

Ministry of Science, Technology, and Innovation (MOSTI)

AI Sandbox pilot programme, collaboration between Higher Education Minister and Nvidia. Aims: 900 startups, 13,000 talents by 2026

Participating in ISO AI Standards development (ISO/IEC 42000)

**SKRINE** Wisdom  
Fortitude  
Ingenuity

## AI Grants / Incentives

**MOSTI**- National AI Strategy, provide indirect support

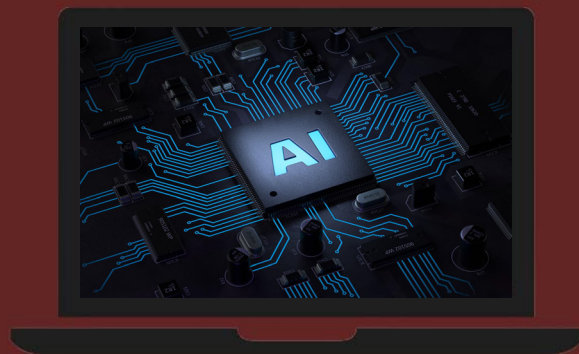
**MDEC** – funding, Digital Transformation Grant,  
Global Innovation and Tech Alliance

**MyDigital Corporation** – initiatives, Malaysian  
Digital Economy Blueprint, National IR4.0 policy

**MyAira** - Malaysian Autonomous Intelligence and  
Robotics Association, non-profit association,  
accelerating innovation in the AI and Robotics sector

**SKRINE** Working  
Towards  
Responsible

## Regulatory Framework for AI in Malaysia



**SKRINE** Working  
Towards  
Responsible



### National Guidelines on AI Governance and Ethics

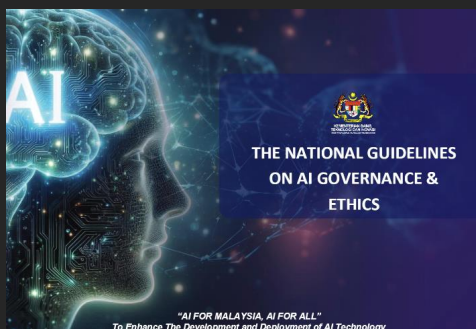
- Developed by MOSTI
- Aimed at 3 use categories: End Users, Policymakers and Developers/Providers of AI
- To ensure AI is used safely, ethically and responsibly.
- Voluntary guidance for industry players whilst the Government develops laws to regulate the use of AI
- Issued on 20 September 2024

### Personal Data Protection Act 2010

- Recently amended by the Personal Data Protection (Amendment) Act 2024
- Has robust data privacy provisions to align with international and GDPR standards
- No specific provisions yet on automated decision making yet
- Profiling and Automated Decision-Making Guidelines intended to be developed

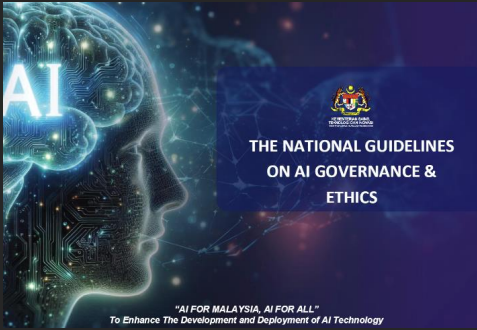
## National Guidelines on AI Governance and Ethics

### Objectives



- To support the implementation of Malaysia’s National AI Roadmap 2021–2025
- To facilitate the implementation of responsible AI, in accordance with the seven AI Principles set out in the Guidelines;
- To build trustworthiness in AI;
- To manage the risks caused by the development and deployment of AI technology; and
- To maximise the benefits of AI to enhance national productivity, economic growth, and competitiveness.

# National Guidelines on AI Governance and Ethics



## Seven AI Principles

- Fairness
- Reliability, safety and control
- Privacy and security
- Inclusiveness
- Transparency
- Accountability
- Pursuit of human benefit and happiness

**SKRINE** WISDOM  
TECHNOLOGY  
INTEGRITY

# Challenges in AI in Malaysia

**SKRINE** WISDOM  
TECHNOLOGY  
INTEGRITY



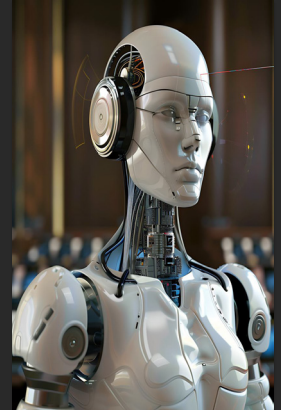
Cost



Data Availability and Quality



Talent and Technical Expertise, Infrastructure Gaps



Regulatory and Ethical Concerns  
*data protection, bias, transparency IP protection*



**Jillian Chia**  
Partner  
[jc@skrine.com](mailto:jc@skrine.com)



...

## Regulatory Landscape for Generative AI in Japan: Insights and Outlook



**Hitomi Iwase**

Attorney, Nishimura & Asahi, Japan



### BIOGRAPHY



Hitomi Iwase is a partner in Nishimura & Asahi's IP/IT practice. She handles patents, copyrights, trademarks, trade secrets, and other IP-related matters across multiple business sectors, including IT, life sciences and healthcare, machinery, food, fashion, environment and energy, entertainment, financial services, and e-commerce. Hitomi's expertise encompasses all forms of IP transactional work, both cross-border and domestic, including licensing, strategic alliances, joint development, and asset transfers, as well as various types of IP disputes, including patent and trademark infringement litigation.

Hitomi regularly advises clients on emerging legal issues related to the latest technology, such as IoT and artificial intelligence (AI), as well as on complex system-related transactions and disputes. In the area of data privacy, Hitomi provides extensive advice on data protection and privacy compliance, including establishing global compliance systems and handling incidents such as data breaches. She also advises on related areas such as e-commerce, advertising, and consumer protection.

# Abstract

Japan's approach to regulating Generative AI is characterized by a soft law framework, while existing laws (such as the Act on the Protection of Personal Information (APPI), the Copyright Act, etc.) apply to the development or use of Generative AI depending on the industry or the nature of the AI. In April 2024, the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry issued the "AI Guidelines for Businesses." These guidelines provide 10 guiding principles, including fairness, transparency, and accountability, as well as practical guidance for AI developers, providers, and users.

This presentation also covers the legal issues surrounding Generative AI, such as potential violations of the APPI and copyright infringement, and examines what platforms need to do to manage the risks associated with developing and providing Generative AI.



# Platform Governance and Generative AI

Japan's regulatory approach to and relevant legal issues surrounding Gen AI

October 18, 2024

**Hitomi Iwase**

## CV



### Hitomi Iwase

Partner | Tokyo  
Tel 81-3 6250 6218  
h.iwase@nishimura.com

Hitomi handles patents, copyrights, trademarks, trade secrets, and other IP-related matters in multiple business sectors, including IT, life sciences and healthcare, machinery, food, fashion, environment and energy, entertainment, financial services, and e-commerce. Ms. Iwase's expertise encompasses all forms of IP transactional work, both cross-border and domestic, including licensing, strategic alliances, joint development, and asset transfers, as well as various types of IP disputes, including patent/trademark infringement litigation. Hitomi also assists clients in anti-counterfeiting and in the development of IP portfolios and prosecution strategies. Hitomi regularly advises clients on emerging legal issues relating to the latest technology, such as IoT and artificial intelligence (AI), as well as on complex system-related transactions and disputes over such transactions. In the area of data privacy, Hitomi provides extensive advice on data protection and privacy compliance, including on establishing global compliance systems and incidents such as data breaches. Hitomi also advises on related areas such as e-commerce, advertising, and consumer protection.

#### Experience

- IP Litigation
- IP Transactions
- Trade Secrets / Unfair Competition
- Anti-Counterfeiting / Brand Management
- IT
- Personal Data & Privacy / Big Data Businesses
- Protection of Commercial Secrets & Customer Information / Cyber Security
- Startups & Venture Capital
- Cross-border Transactions (General)
- International Litigation



“ She always works very, very well and has very high professionalism. ”

Technology, Media, Telecoms (TMT) in Japan  
Chambers Asia-Pacific 2024

**Hitomi is a partner in the firm's IP/IT practice and heads the trademark/design team. She covers all aspects of intellectual property (IP), information technology (IT), and data privacy and advises both Japanese and international clients on disputes and transactions in related areas.**

#### Awards

- Chambers Asia-Pacific (Intellectual Property) (2019-2024)
- Chambers Global (Intellectual Property: Domestic) (2020-2024)
- The Legal 500 Asia Pacific (Intellectual Property) (2020-2024)
- Who's Who Legal: Global (Patents) (2023)
- IAM Strategy 300 - The World's Leading IP Strategists (2023)
- Women in Business Law Awards Asia-Pacific (2022-2023)
- Managing IP - The Top 250 Women in IP (2023)
- Asian Legal Business - Top 15 Intellectual Property Lawyers in Asia (2022)
- Asia IP Experts (Patents, Trademarks, Enforcement, IP Litigation, IT & Telecoms) (2021)
- Top attorneys in Japan: Best Lawyers - 2021 edition (Intellectual Property) (2020)
- World Trademark Review Global Leaders (2019-2023)
- IAM Patent 1000 - The World's Leading Patent Professionals (2019-2023)
- World Trademark Review 1000 - The World's Leading Trademark Professionals (2019-2022)

#### Education

- Waseda University (LL.B.)
- Stanford Law School (LL.M.)

#### Publications

- 2023 Japan Chapter, World Trademark Review Yearbook 2022/2023 (Globe Business Media Group)
- 2022 Practical Law Global Guide 2022: Intellectual Property Transactions - Japan (Practical Law Global Guide)
- 2020 Revisions to Japan Copyright Act to tackle online pirating (International Law Office Newsletter)
- 2020 IP in Business Transactions - Japan, Practical Law IP in business transactions Global Guide 2020 (Practical Law Global Guide)
- 2020 Corpus Juris Series - Personal Information Protection Legislation (Global) (Shojihomu Co., Ltd.)
- 2020 Amendments to the Act on the Protection of Personal Information in 2020 and Practical Approaches (Shojihomu Co., Ltd.)



## Soft Law Approach

- ▶ No hard law that specifically regulates or addresses AI or Generative AI
- ▶ **“AI Guidelines for Business Ver1.0” (April 19, 2024, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)**
  - ▷ Main part: 35 pages, Appendix: 157 pages
  - ▷ Guidance to AI developers, AI providers, AI users
  - ▷ English translation
- ▶ **AI Strategy Council (AI戦略会議)**
  - ▷ Draft Discussion Points
  - ▷ Safety, privacy and fairness, national security and crime, property protection, and intellectual property
- ▶ **“Basic Act on the Advancement of Responsible AI” Bill(責任あるAI推進基本法)**

2



## AI Guidelines for Business Ver1.0

Main Appx.  
Preface

### Basic Concept of “AI Guidelines for Business”

- The basic concepts of “AI Guidelines for Business” are **1** Support for voluntary efforts by business operators, **2** Coordination with international discussions, and **3** Understandability for readers.
- In addition, the Guidelines will continue to be updated as a “Living Document” through continuous “multiple stakeholder” reviews and with an emphasis on effectiveness and legitimacy.

#### Concepts



#### Processes

**Multiple stakeholders**  
Established through studies conducted by multiple stakeholders that consisted of academic and research institutions, civil societies including general consumers, private sector companies, and the like, to prioritize effectiveness and validity.

**Living Document**  
To continuously improve AI governance, updated as needed while reflecting the agile governance philosophy.

[https://www.meti.go.jp/shingikai/mono\\_info\\_service/ai\\_shakai\\_jisso/pdf/20240419\\_10.pdf](https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240419_10.pdf)

3





## AI Guidelines for Business Ver1.0

Main Appx.

### Common Guiding Principles for All Actors

**Part 2**

- The "Common Guiding Principles" outlines what each actor works on in collaboration to achieve the society aimed for through AI.
- The "Common Guiding Principles" are formulated based on the "Social Principles of Human-Centric AI," integrating three guidelines in Japan with consideration of trends in other countries and the emergence of new technologies.
- As a result, it is organized into what each actor works on and what is expected to be worked on in collaboration with society.

Social Principles of Human-Centric AI	Recommendation on the Ethics of Artificial Intelligence
AI Utilization Guidelines	Blueprint for an AI Bill of Rights
AI R&D Guidelines	AI RMF 1.0
Governance Guidelines for Implementation of AI principles	The G7 Digital and Tech Ministers' Meeting
Ethics guidelines for trustworthy AI	The Hiroshima AI Process Guiding Principles/ Code of Conduct
Recommendation of the Council on Artificial Intelligence	

Extract and organize common elements

Activities to be implemented by each AI business actor

1) Human-Centric	2) Safety	3) Fairness
4) Privacy protection	5) Ensuring security	
6) Transparency	7) Accountability	

Activities to be implemented in cooperation with society

8) Education/literacy	9) Ensuring fair competition	10) Innovation
-----------------------	------------------------------	----------------

[https://www.meti.go.jp/shingikai/mono\\_info\\_service/ai\\_shakai\\_jisso/pdf/20240419\\_10.pdf](https://www.meti.go.jp/shingikai/mono_info_service/ai_shakai_jisso/pdf/20240419_10.pdf)

## Soft Law Approach

- ▶ No hard law that specifically regulates or addresses AI or Generative AI
- ▶ **"AI Guidelines for Business Ver1.0"** (April 19, 2024, Ministry of Internal Affairs and Communications and Ministry of Economy, Trade and Industry)
  - ▷ Main part: 35 pages, Appendix: 157 pages
  - ▷ Guidance to AI developers, AI providers, AI users
  - ▷ English translations
- ▶ **AI Strategy Council (AI戦略会議)**
  - ▷ Draft Discussion Points
  - ▷ Safety, privacy and fairness, national security and crime, property protection, and intellectual property
- ▶ **"Basic Act on the Advancement of Responsible AI" Bill (責任あるAI推進基本法)**

## Other Laws Affecting AI/Generative AI

- ▶ **Copyright Act and other IP laws**
  - ▷ "General Understanding on AI and Copyright in Japan" (March [ ], 2024, (Legal Subcommittee under the Copyright Subdivision of the Cultural Council)
  - ▷ "Interim Report of the expert group on Intellectual Property Rights in the AI Era" (May 2024)
- ▶ **Data privacy: The Act on the Protection of Personal Information (APPI)**
  - ▷ Warning (Cautions) to a Generative AI platform (June 1, 2023)
  - ▷ Cautionary notice regarding the use of Generative AI services (June 2, 2023)
- ▶ **The Information Distribution Providers Act(情報流通プラットフォーム対処法) (the 2024 amendment to the existing Providers' Liability Limitation Act)**
  - ▷ Aims to expedite content takedown requests.
- ▶ **The Digital Platform Transparency Act(特定デジタルプラットフォーム取引透明化法) (entered into force in 2021)**
  - ▷ Requires large online malls, app stores, and digital advertising businesses to ensure transparency and fairness in transactions with business users
- ▶ **The Civil Code**
- ▶ **The Criminal Code, ETC.**

6



## Copyright Act



### Overview of the General Understanding : AI Development / Training Stage



#### Article 30-4 of the Copyright Act

- **Exploitation of a copyrighted work not for enjoyment of the thoughts or sentiments expressed in the copyrighted work (exploitation for non-enjoyment purposes)\*** such as AI development or other forms of data analysis may, in principle, be allowed without the permission of the copyright holder. \*e.g., collection (i.e. reproduction) of copyrighted works as AI training data
- **"Enjoyment"** under the Article 30-4 refers to the act of **obtaining the benefit of having the viewer's intellectual and emotional needs satisfied through using the copyrighted work.**

《Examples of acts that can be called "enjoyment"》

Literary works	: To read	Musical works	: To appreciate
Works of computer programming	: To execute	Movie works	

- The financial benefits that copyright holders receive from their works are generally considered rewards for meeting intellectual and emotional needs. Meanwhile, the **exploitation of works for non-enjoyment purposes, which may occur without the consent of the copyright holder**, is generally regarded as not harming the financial interests of the copyright holder. Therefore, in such cases acquiring permission for use of the copyrighted works from the copyright holder is not deemed to be required pursuant to Article 30-4 of the Act.

[https://www.bunka.go.jp/english/policy/copyright/pdf/94055801\\_01.pdf](https://www.bunka.go.jp/english/policy/copyright/pdf/94055801_01.pdf)

7

## Copyright Act



### Overview of the General Understanding : AI Development / Training Stage



#### Article 30-4 of the Copyright Act

- ❑ The provisions of Article 30-4 of the Act do not apply to the "exploitation of works for the purpose of enjoyment" and the "exploitation of works where the main purpose is non-enjoyment such as provision for use in data analysis, but where there is also the purpose of enjoyment.\*"

\* The presence or absence of an "enjoyment" purpose is determined by "the work" exploited under the Article, not by other copyrighted works or not copyrighted elements such as an "artist's style".

- ❑ Where a work is being used for "non-commercial" or "research purposes", etc., permission from the copyright holder is required where there is also a "purpose of enjoyment" of the work present.
- ❑ Furthermore, Article 30-4 of the Act does not apply in "cases that would unreasonably prejudice the interests of the copyright holder.\*"

• e.g., reproducing a copyrighted database work for the purpose of data analysis, such as AI training for which licenses for data analysis are available in the marketplace, etc.

[https://www.bunka.go.jp/english/policy/copyright/pdf/94055801\\_01.pdf](https://www.bunka.go.jp/english/policy/copyright/pdf/94055801_01.pdf)

8

## Other Laws Affecting AI/Generative AI

- ▶ **Copyright Act and other IP laws**
  - ▷ "General Understanding on AI and Copyright in Japan" (March [ ], 2024, (Legal Subcommittee under the Copyright Subdivision of the Cultural Council)
  - ▷ "Interim Report of the expert group on Intellectual Property Rights in the AI Era" (May 2024)
- ▶ **Data privacy: The Act on the Protection of Personal Information (APPI)**
  - ▷ Warning (Cautions) to a Generative AI platform (June 1, 2023)
  - ▷ Cautionary notice regarding the use of Generative AI services (June 2, 2023)
- ▶ **The Information Distribution Providers Act(情報流通プラットフォーム対処法) (the 2024 amendment to the existing Providers' Liability Limitation Act)**
  - ▷ Aims to expedite content takedown requests.
- ▶ **The Digital Platform Transparency Act(特定デジタルプラットフォーム取引透明化法) (entered into force in 2021)**
  - ▷ Requires large online malls, app stores, and digital advertising businesses to ensure transparency and fairness in transactions with business users
- ▶ **The Civil Code**
- ▶ **The Criminal Code, ETC.**

9





**Nishimura & Asahi (Gaikokuho Kyodo Jigyo)**

Otemon Tower, 1-1-2 Otemachi, Chiyoda-ku, Tokyo

100-8124, Japan

Tel +81 36250 6200



Day  
**2**

# Session 5

## What is Data Sovereignty? Global Cross-border Privacy Rules (GCBPRs) and Cooperation in Investigation and Enforcement

### Chair

Kwang Bae PARK  
Attorney, Lee & Ko, Republic of Korea



### 1

Jeongsoo LEE  
Deputy Director, Personal Information Protection  
Commission, Republic of Korea



### 2

Huyen-Minh Nguyen  
Senior Associate, BMVN International LLC, Vietnam



### 3

Dominic Edmondson  
Special Counsel, Baker McKenzie, Hong Kong







## South Korea's Regulatory Framework for Cross-Border Data Transfer Policies



Jeongsoo LEE

Deputy Director, Personal Information Protection Commission,  
Republic of Korea



### BIOGRAPHY



Jeong-soo is a data protection and privacy policy expert at the Personal Information Protection Commission (PIPC) in South Korea. In her current role, she focuses on cross-border data transfer policy, engaging in activities ranging from planning amendments to legislation to negotiating with data protection authorities worldwide, including the European Union. Jeongsoo is also responsible for implementing the Korean adequacy system, which was established in September 2023.

Prior to joining the PIPC, she worked at the Korean Communications Commission (KCC), where she specialized in data protection and international cooperation initiatives, including the APEC Cross-Border Privacy Rules (CBPR), EU Adequacy, and various other international commitments.

# Abstract

In this presentation, you can expect a comprehensive introduction to Korean legislation concerning cross-border data transfers. It begins with a brief historical overview of the legislative framework, followed by an explanation clarifying the scope and application. Additionally, the presentation details the amended legislation enacted in September 2023, which enhances the mechanisms for safe cross-border transfers. This includes provisions for certification and equivalency recognition, which form part of Korea's adequacy system. Furthermore, the presentation explores potential future developments in cross-border transfer regulations, considering the increasing global demand for such transfers.



# Cross-border Transfer Policy in South Korea

October 18, 2024

Jeongsoo Lee / Deputy Director

Personal Information Protection Commission(PIPC)



## Contents

- 1 **Brief History of Cross-border Transfer Regulation**
- 2 **How to protect the 'cross-border data transfer'?**
- 3 **Scope of the Application (PIPA vs FSA)**
- 4 **5 ways for Cross-border Transfer from Korea**
- 5 **Going Forward (More ways)**

## 1. Brief History

- Stage 1 (~2020) : Separated Laws
  - Personal Information Protection Act, Network Act, Financial Service Act... etc.
- Stage 2 (2020~2023) : One law, Two rules
- Stage 3 (2023~ ) : One law, One rule + More ways of Transfer
- ➔ ▪ Stage 4(?) : More flexibility, but maintain safe protection

1

## 2. How to protect 'cross-border transfer'

① **Why additional protection on Cross-border transfer needed?** → Risks of being transferred to the new jurisdiction with different level of data protection

② **'Risk' should be controlled and minimized**  
→ Proper safeguard should be taken before transfer is allowed, and data subject shall be noticed of the cross-border transfer

③ **Protection after transfer**  
→ PIPC can take action on transfers with violation, and may order the suspension of data transfer, but as a final resolution

### 3. Scope of Application in Korea

- In which case PIPA or Credit Information Act(CIA) applies:
  1. "Personal Credit Information" falls under CIA / supervised by FSC
  2. PIPA as a general law, it applies when FSA does not regulate (§3 CIA)
  3. Cross-data Transfer : PIPA applies (Every Personal Information including PCI)
- Scope of Application:

	Personal Information (except Personal Credit Information)	Personal Credit Information
General Rule (Collection, use, third-party provision...)	PIPA	CIA
Cross-border Data Transfer	PIPA	NO rule in CIA → PIPA

4

### 4. 5 Ways for Cross-border Transfer

#### ❖ Mechanisms for transfer (Sep 2023)

- Data Subject Consent :  
The consent should be separate with other consents, and freely given.
- Special rules in specific laws
- Entrustment/Storage which are necessary for concluding/implementing contract with Data Subject
- (NEW) Certification (recognized by the PIPC)
- (NEW) Equivalency of the protection level (recognized by the PIPC)  
: Korean "Adequacy" System (similar with the EU one)

5

## 4. 5 Ways for Cross-border Transfer

### ❖ Korean 'Adequacy' Decision

- 'Essentially equal level of protection' → Transfer to that jurisdiction
- Criteria for Adequacy/Equivalency Assessment
  1. Principles of data protection & Data subject rights guarantee
  2. Independent supervisory authority
  3. Legitimate basis/redress of Government Access (by public institution)
  4. Effective redress mechanism for Korean data subject
  5. Data Protection Authority which can mutually cooperate with the PIPC
- PIPC Secretariat – Expert Committee – Related agencies – PIPC

5

## 5. Going Forward (more ways)

### ❖ Consideration of more ways

- Standards Contractual Clause (SCC)
- Binding Corporate Rules (BCRs)
- Consideration of the exceptional cases for public purposes  
(e.g. public health, public security, inter-government cooperation...)
- Reconsideration of the role of the 'data subject consent'

6

...

## Data Sovereignty in Vietnam: Legal Requirements, Enforcement Trends, and Global CBPRs Interactions



Huyen-Minh Nguyen  
Senior Associate, BMVN International LLC, Vietnam

### ▼ BIOGRAPHY 🔍

Huyen-Minh is a senior associate in the Intellectual Property and Technology practice in Vietnam. She possesses in-depth expertise in advising both foreign and local companies on navigating the complexities and uncertainties of evolving and divergent local data privacy laws, as well as identifying vulnerabilities and recommending robust data protection policies to ensure compliance with prevailing regulations and industry standards. She is also an active policy advocate in the areas of data protection, cybersecurity, and technology, with a worldview and cultural nuances informing her policy approach.

Huyen-Minh's clients span diverse industries, including banking and finance, payment services, insurance, technology, food and beverages, manufacturing, and retail.

# Abstract

Imposing data localization requirements is one way Vietnam asserts its sovereignty over data. The first data localization requirement was introduced in Vietnam under the Cybersecurity Law of 2016, which broadly applies to all offshore and onshore enterprises providing services on the Internet and processing certain data generated by and pertaining to service users in Vietnam. However, due to a lack of guidance from local authorities and the absence of a legal mechanism to enforce it, the requirement remained unenforceable for years. In 2022, the Government issued Decree 53 to clarify the data localization requirements under the Cybersecurity Law of 2016. Decree 53 significantly limits the cases in which companies are required to localize their data in Vietnam, with different sets of triggering conditions applying to offshore and onshore enterprises.

This presentation discusses the requirements of the Cybersecurity Law of 2016, Decree 53, and enforcement trends over the last few years. It also explores several new regulations that attempt to introduce additional cross-border data restrictions, such as the Data Law and the draft decree guiding the Law on Telecommunications, and how these may interact with or hinder the application of Global Cross-border Privacy Rules in Vietnam.

# BMVN.

## Data Sovereignty in Vietnam Legal Requirements, Enforcement Trends, and Global CBPRs Interactions

Huyen-Minh Nguyen | November 2024

### DATA LOCALIZATION vs. DATA SOVEREIGNTY

#### Data Localization

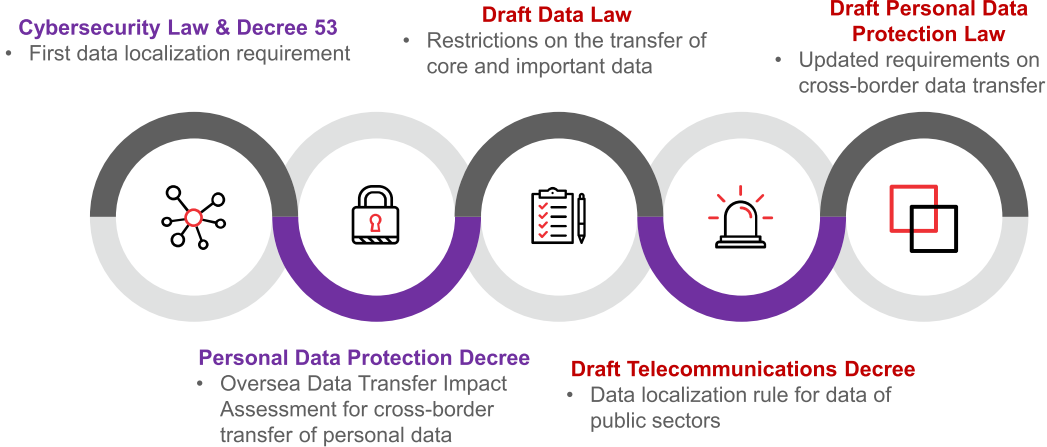
- Requiring data to be stored and processed locally.
- Different levels of “localization”
  - Restrictions on data transfer;
  - Data mirroring;
  - Local-only storing.
- Purposes?



#### Data Sovereignty

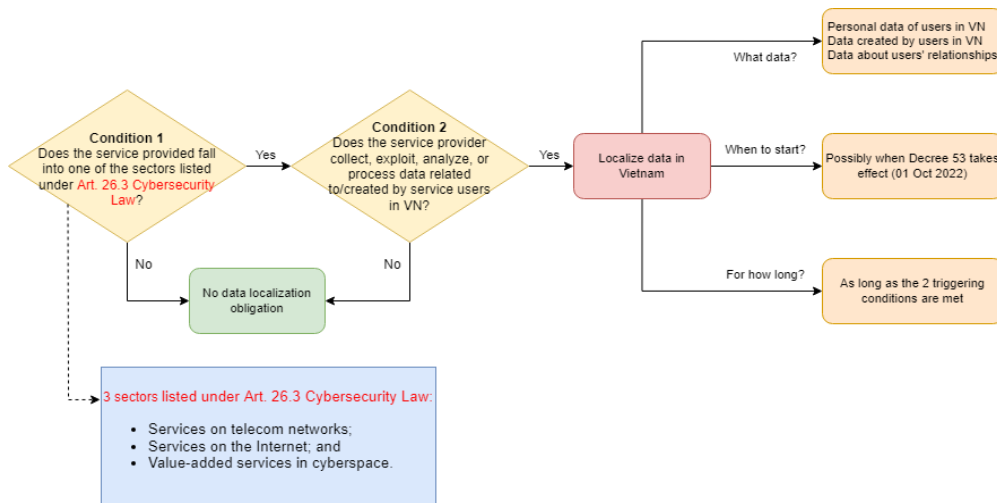
- The “concept” - no unified definition.
- Which jurisdictions and governance mechanisms that a set of data may be subject to?

## EVOLVING VIETNAM REGULATORY LANDSCAPE



## CYBERSECURITY LAW & DECREE 53

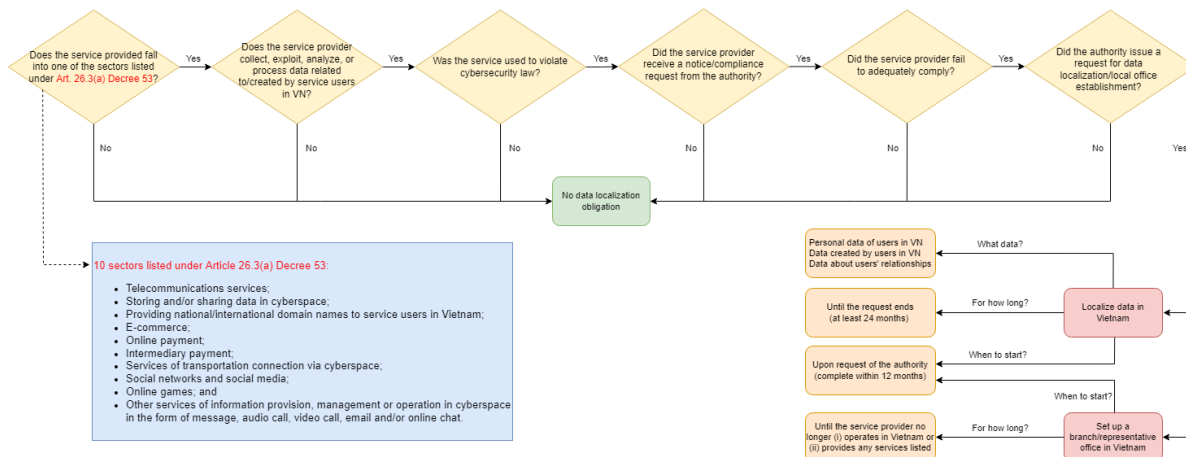
### Data localization & local office requirements - Onshore enterprises





# CYBERSECURITY LAW & DECREE 53

## Data localization & local office requirements - Offshore enterprises



# PERSONAL DATA PROTECTION DECREE



No **prior approval** of the competent authority is required



Submit an **Overseas Data Transfer Impact Assessment (OTIA)** to the Ministry of Public Security (MPS); notify the contact details to the MPS



Comply with **the requirements of the MPS** on updating & amending the dossier

## PERSONAL DATA PROTECTION DECREE

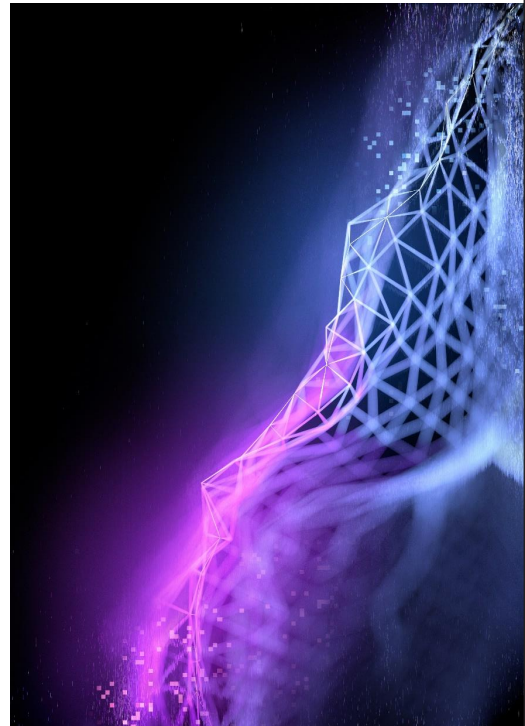


The new OTIA require **substantially detailed information** on:

- Corporate details (e.g., tax code, address, branch, rep person and office, business line, DPO)
- Contracted data processors / data importers / third parties / onward transfers
- Description of data processing (e.g., estimated number of data subjects, amount of personal data, retention period)
- Risks and corresponding mitigation measures



**Data processing / transfer agreements** must be translated and submitted.



## DRAFT PERSONAL DATA PROTECTION LAW

Released for public consultation (2 months)



24 Sept 2024

May 2025



Tentative Issuance Date

Tentative Effective Date



1 Jan 2026



### Cross-border data transfer

- Requirements on Overseas Data Transfer Impact Assessment remain.
- Clarifications on cases that are considered “cross-border transfer” of personal data.

## DRAFT DATA LAW & DRAFT TELECOMMUNICATIONS DECREE



### Draft Data Law

- The Draft Law proposes to regulate “core data” and “important data”
- A decision from the Prime Minister or the MPS is required before transferring those types of data outside of Vietnam, respectively.
- The data owner must obtain a data security assessment conducted by the MPS and sign a contract with the foreign data recipient according to a standard contract developed by the MPS before transferring core data or important data.



### [Draft] Telecommunications Decree

- Data of state agencies using data center and/or cloud computing services shall only be stored in Vietnam
- Enterprises providing data center and cloud computing services to state agencies must meet requirements on the safety of the information system

## ANY PENALTY FOR NON-COMPLIANCE?



### Monetary fine?

No specific fine for now.



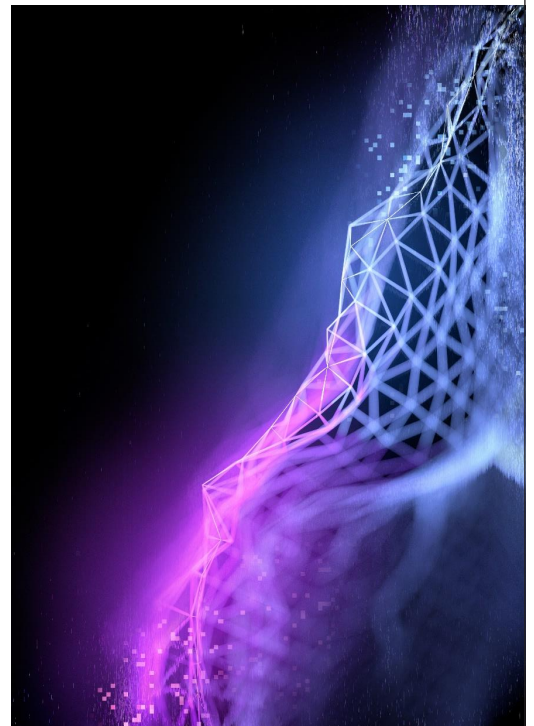
### Other enforcement actions?

The cross-border data transfer can be suspended if the data exporter fails to update the OTIA.



### Draft CASD?

Monetary fine up to 5% of the offender's total revenue of the preceding fiscal year in Vietnam; license revocation; processing cessation; data destruction; confiscation of means; etc.



## GLOBAL CROSS-BORDER PRIVACY RULES (GCBPRS)



### A regional / global framework to support the effective protection and flow of data internationally

- No data localization / jurisdictional-specific requirements



### Possible approaches?

- Contractual clauses (ASEAN MMCs)
- Certifications (APEC/Global CBPR Certifications)



### Challenges

- Uncertain legal effect. Vietnam has yet recognized ASEAN MMCs / CBPR Certifications as a valid legal basis for cross-border data transfer

### Baker McKenzie delivers integrated solutions to complex challenges.

Complex business challenges require an integrated response across different markets, sectors and areas of law. Baker McKenzie's client solutions provide seamless advice, underpinned by deep practice and sector expertise, as well as first-rate local market knowledge. Across more than 70 offices globally, Baker McKenzie works alongside our clients to deliver solutions for a connected world.

[bakermckenzie.com/bmvm/](https://bakermckenzie.com/bmvm/)

This presentation has been prepared for clients and professional associates of Baker & McKenzie. Whilst every effort has been made to ensure accuracy, this presentation is not an exhaustive treatment of the area of law discussed and no responsibility for any loss occasioned to any person acting or refraining from action as a result of material in this presentation is accepted by Baker & McKenzie.

BMVN International LLC is a member firm of Baker & McKenzie International, a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organisations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.  
© 2024 BMVN International LLC

...

## Global Cross-Border Transfers: A Comparative Analysis of China, Hong Kong, and Beyond



**Dominic Edmondson**  
Special Counsel, Baker McKenzie, Hong Kong



### BIOGRAPHY



Dominic Edmondson is a special counsel in Baker McKenzie's Hong Kong office and a member of the Firm's Intellectual Property Practice Group. His practice focuses on global data privacy and data protection, information technology advisory work, IT sourcing and transactions, cybersecurity, e-commerce, telecommunications, and digital media, as well as both contentious and non-contentious intellectual property matters. He works with clients across all sectors, particularly in technology, media and telecommunications, automotive, financial services, consumer goods and retail, and healthcare and life sciences. As a Mandarin speaker, Dominic spent four years advising clients on intellectual property strategy and enforcement in Mainland China (Beijing) before moving to Hong Kong to expand his practice to include data privacy and technology transactions. He is admitted to practice law in England and Wales and in Hong Kong.

Dominic has a keen interest in AI, big data, and distributed ledger technology, and their impact on business in the Greater China region and more broadly in Asia. He has recently been advising clients on their AI governance strategies.

# Abstract

This presentation focuses on the challenges of enabling cross-border data flows while complying with data sovereignty laws. First, the discussion covers how conflicting laws across countries can complicate data transfers and analyzes data localization requirements in various countries, such as China. Next, it analyzes the effectiveness of Global Cross-Border Privacy Rules (GCBPRs) in facilitating cross-border data transfers and explores the challenges of achieving widespread adoption, using the APEC Cross-Border Privacy Rules (CBPR) system as an example. The presentation examines its role in enabling secure data flows while protecting privacy and provides examples of how this system has been used by participating countries.



## Agenda

- 01 Introduction to Data Sovereignty and Data Localization
- 02 APAC Jurisdictions with Data Sovereignty and Localization Laws
- 03 Cross-Border Data Transfer (CBDT) Standard Contractual Clauses in APAC
- 04 Cross-Border Privacy Rules (CBPRs)
- 05 CBDT for Investigation and Enforcement
- 06 Key Takeaways

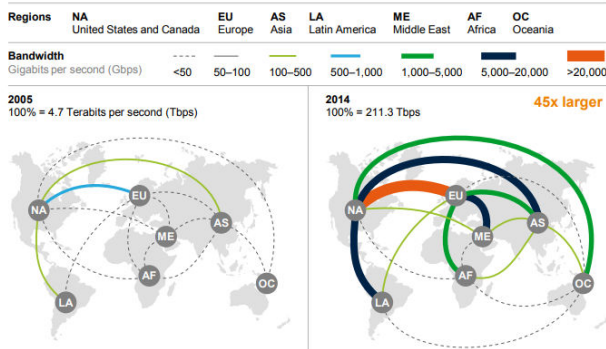


# 01 Introduction to Data Sovereignty and Data Localization

## An Illustration of Modern Data Flow

Cross-border data flows are surging and connecting more countries

Used cross-border bandwidth



Source: Changes in Global Data Flow Between Regions Source: McKinsey Global Institute. (2016, March)





## Data Sovereignty vs Data Localization

### Data Sovereignty:

- A broad concept that data collected, processed, or stored in a particular jurisdiction should be subject to the laws of that jurisdiction
- Focused on the jurisdiction's legal grip on the data

### Data Localization:

- The practice of storing, processing and using the data within the geographical boundaries of the originating geographic location
- Focused on the jurisdiction's physical grip on the data
- A strict approach to data sovereignty

5

## 02 APAC Jurisdictions with Data Sovereignty and Localization Laws

## Selected APAC Jurisdictions

Jurisdiction	Consent	Risk Assessment	Regulatory Approval	Overseas Privacy Safeguards	Localization
Australia	✓			✓	✓
China	✓	✓	✓	✓	✓
Hong Kong					
Indonesia	✓			✓	✓
Japan	✓		✓	✓	
Malaysia	✓			✓	
Singapore	✓		✓	✓	
South Korea	✓			✓	✓

Please refer to Baker McKenzie's Global Data Privacy and Cybersecurity Handbook for details  
(<https://resourcehub.bakermckenzie.com/en/resources/global-data-privacy-and-cybersecurity-handbook>)

7

## 03 Cross-Border Data Transfer (CBDT) Standard Contractual Clauses in APAC

## Overview of CBDT Standard Contractual Clauses (SCCs)



Pre-approved model contractual clauses that are to be adopted or can be incorporated into the underlying commercial agreement between the transferor and the recipient



### Purposes

- To satisfy the legal requirement of CBDT of ensuring the overseas recipient to protect the data by the same standards as those imposed by the originating jurisdiction
- To simply compliance, as entering into SCC is often an alternative mechanism to other more stringent requirements (e.g., obtaining regulatory approval)

9

## Notable APAC Jurisdictions with SCCs

### China

- Only open to smaller and non-critical businesses
- Non-amendable

### Hong Kong


- SCCs are recommended only as the statutory provision on cross-border data transfer is not currently in force
- Specific SCCs are recently published for data transfer within the Greater Bay Area

### ASEAN

- Applicable to data transfers from and/or within ASEAN countries
- Modular approach (similar to EU SCC)
- May be amended to suit business needs so long as the amendment is consistent with the principles of the ASEAN Framework on Personal Data Protection

10

## Other APAC Jurisdictions with SCCs

 <p>Australia (no national SCCs, state-level SCCs only)</p>	 <p>New Zealand</p>	 <p>Philippines (no national SCCs, but encourages businesses to adopt international SCCs)</p>	 <p>Thailand (no national SCCs, and parties must adopt international SCCs with specific regulatory modifications)</p>
--	--	--	--

11

## 04 Cross-Border Privacy Rules (CBPRs)

## What are CBPRs?

A voluntary, data privacy certification that companies can use to certify their global operations through a single process

Includes certification processes for businesses, ensuring they adhere to the privacy principles outlined in the framework

The privacy practices of companies certified under the CBPR system carry a seal of compliance that is recognizable across participating CBPR economies

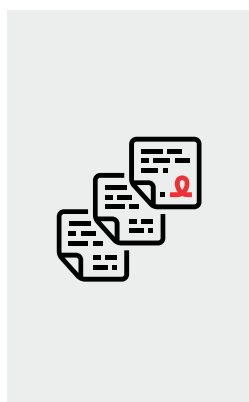


### Benefits

- Ensure the appropriate level of privacy protection for personal data
- Promote consistent baseline protections across jurisdictions
- Builds consumer trust in data transfers

13

## Examples of CBPRs












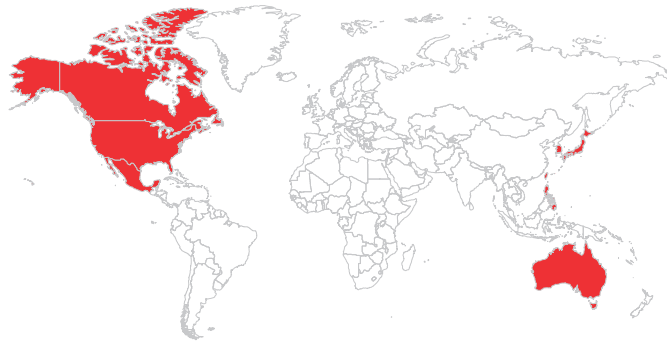
- Organisation for Economic Co-operation and Development (OECD) Privacy Guidelines
- Asia-Pacific Economic Cooperation (APEC) CBPR system
- Global CBPR system
- ASEAN Framework on Personal Data Protection
- General Data Protection Regulations (GDPR) (within EU/UK)
- US Data Privacy Framework (DPF)
  - EU-US DPF
  - UK Extension to the EU-US DPF
  - Swiss-US DPF

14

# APEC CBPR System

Participating economies:

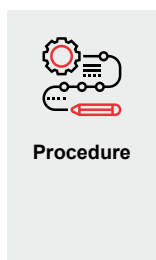
-  Canada
-  Chinese Taipei
-  Japan
-  USA
-  South Korea
-  Mexico
-  Philippines
-  Australia
-  Singapore



15

# APEC CBPR System

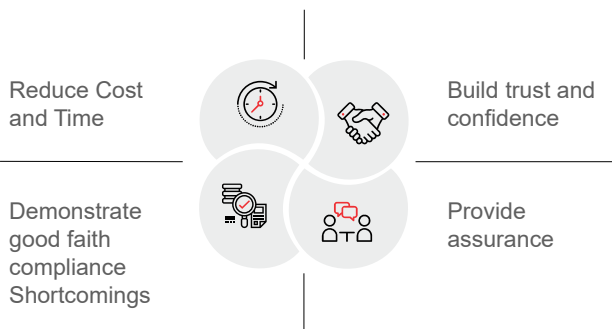
- A voluntary, enforceable, international, accountability-based system that is based on the APEC Privacy Framework
- Requires data controllers to implement data privacy policies consistent with the APEC Privacy Framework
- Aim: facilitate compliant and safe cross-border data transfers between participating economies
- Enforced by individual countries' privacy enforcement authorities



16

## APEC CBPR System

### Benefits



17

## APEC CBPR System

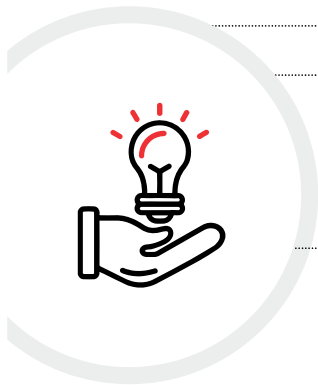
### Questionable Effectiveness (according to APEC Business Advisory Council Singapore)



- Low participation by countries and businesses
  - Only 9 out of 21 APEC economies are participating in CBPR
  - Only 5 economies have fully implemented the system in their jurisdictions with the appointment of Accountability Agents
  - Only slightly more than 60 companies have been CBPR certified
- Low awareness by small businesses
- Low recognition as an adequate transfer mechanism in law
- Most businesses prefer the alternative mechanisms (e.g., SCCs)
- Non-alignment with international privacy frameworks (e.g., GDPR)

18

## Solution: Global CBPR System



- Current progress: Creation of a Global CBPR Forum
- Aims of the Forum
  - Establishment of an international certification system based on APEC CPBR
  - Promoting interoperability with other data protection and privacy frameworks
- Potential future steps
  - Better alignment between CBPR requirements with GDPR (i.e., obtaining EU approval of the CBPR as an adequate data protection measure)
  - Amendment of local laws to expressly recognize the legal status of CBPR certifications

19

## 05 CBDT for Investigation and Enforcement



## Hong Kong's CBDT Legal Framework for Investigations



- No specific CBDT provisions in force
- Data Protection Principle 3 under the Personal Data (Privacy) Ordinance (PDPO): personal data is only used for the purpose for which the data is collected (unless consent is obtained)
- Exemptions
  - Use for safeguarding security, defence or international relations for HK
  - Use for prevention and detection of crimes in HK, or apprehension or prosecution of offenders of crimes in HK
    - Exception to the exception: cross-border law enforcement cooperation
  - Use in legal proceedings in HK or for exercising or defending legal rights in HK
- No generally applicable exemptions for crime/legal rights outside of HK
- Implications: insert appropriate investigation and enforcement clause in the data collection statement to expressly cover overseas crimes, rights and proceedings

21

## China's CBDT Legal Framework for Investigations



- Under the Cybersecurity Law (CL) and Personal Information Protection Law (PIPL), without the approval of competent authorities, personal information controllers shall not provide any personal information stored within China to a foreign judicial or law enforcement body
- Chinese authorities will handle foreign law enforcement or judicial assistance requests for personal information in China on a case-by-case basis, based on:
  - Applicable laws or treaties
  - The principle of equality and reciprocity
- Uncertainties
  - Which government department or court is the "competent authority"?
  - What is the application procedures

22

## Conflict of Laws



- Some jurisdictions may have laws compelling transfer of data stored overseas for law enforcement or litigation purposes
- Overseas jurisdiction may expressly prohibit/have no exemption for CBDTs for such purpose

23

## Conflict of Laws – Case Studies

### Google Warrant Case (2017) in USA

- The Court ordered Google to produce account data in servers outside the US to FBI for use in criminal investigations
- What if the data is stored in China which prohibits CBDT even for law enforcement purposes (unless specifically approved)?

### New Frontier Case (2024) in Cayman Islands

- New Frontier was a party to a Cayman Island litigation and was ordered to disclose numerous corporate documents stored in China
- New Frontier sought an indefinite extension of time for disclosure as there is no mechanism for obtaining Chinese approval under PIPL and the Cybersecurity Law
- The Court acknowledged that the restrictions in CL and PIPL are engaged, and New Frontier faced a "low to moderate" risk of prosecution in the PRC
- However, the Court refused to grant the extension despite the risks

24



## Practical tips

Navigating Through Various CBDT Regimes



### Check the Applicable Laws

- For data usage that crosses national borders, check the local data sovereignty laws in all jurisdictions through which the data passes
- More often than not, there will be data localization laws, especially for sensitive data



### Use Standard Contractual Clauses

- Most jurisdictions allow for CBDT upon satisfactory privacy safeguards on the recipient's usage of data
- SCCs are helpful tools (if not necessary) to demonstrate compliance

# Practical tips

## Navigating Through Various CBDT Regimes



### Use of CBPR Certifications

- CBPR requirements in different multi-jurisdictional arrangements are often similar but different
- Certification does not necessarily equate to compliance
- Consider the costs of certification



### Be Cautious with CBDT Requests for Investigations

- Check whether local laws permit the disclosure for such purposes
- Check the procedure of disclosure, particularly whether regulatory approval is required
- Consider potential conflicts of laws

27

**Baker McKenzie delivers integrated solutions to complex challenges.**

Complex business challenges require an integrated response across different markets, sectors and areas of law. Baker McKenzie's client solutions provide seamless advice, underpinned by deep practice and sector expertise, as well as first-rate local market knowledge. Across more than 70 offices globally, Baker McKenzie works alongside our clients to deliver solutions for a connected world.

[bakermckenzie.com](https://www.bakermckenzie.com)

This presentation has been prepared for clients and professional associates of Baker & McKenzie. Whilst every effort has been made to ensure accuracy, this presentation is not an exhaustive treatment of the area of law discussed and no responsibility for any loss occasioned to any person acting or refraining from action as a result of material in this presentation is accepted by Baker & McKenzie.

Baker & McKenzie, a Hong Kong Partnership, is a member firm of Baker & McKenzie International, a global law firm with member law firms around the world. In accordance with the common terminology used in professional service organisations, reference to a "partner" means a person who is a partner, or equivalent, in such a law firm. Similarly, reference to an "office" means an office of any such law firm. This may qualify as "Attorney Advertising" requiring notice in some jurisdictions. Prior results do not guarantee a similar outcome.

© 2024 Baker & McKenzie

Day  
**2**

# Session 6

## Fair Use of Data

### Chair

Byungnam LEE

Senior Advisor, Kim & Chang, Republic of Korea



### 1

Joseph Hyun-Tae Kim

Associate Professor, Yonsei University,  
Department of Applied Statistics, Republic of Korea



### 2

Hyun Joon Kwon

Former Director, Personal Data Secure Usage Division,  
Korea Internet & Security Agency, Republic of Korea







## Exploring Utility and Privacy in Synthetic Data



**Joseph Hyun-Tae Kim**

Associate Professor, Yonsei University,  
Department of Applied Statistics, Republic of Korea



### BIOGRAPHY



Joseph Hyun-Tae Kim is a Professor in the Department of Statistics and Data Science at Yonsei University and serves as the CEO of Greta Inc. He is the Principal Investigator of the BK21 research group 'Interdisciplinary data science education and research based on big data' at Yonsei University. Professor Kim also holds the position of Associate Dean at the Graduate School of Economics and is the Director of the Institute of Data Science at Yonsei University. He earned his Ph.D. in Actuarial Science from the University of Waterloo in Canada and completed his undergraduate studies with a BS in Statistics from Seoul National University in Korea. With his extensive academic background and leadership roles, Professor Kim contributes significantly to the fields of statistics, data science, and interdisciplinary research.

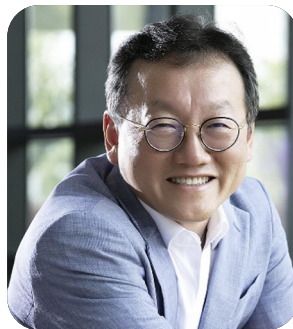
# Abstract

Synthetic data is becoming increasingly popular as a valuable resource for data-driven decision-making and machine learning, particularly especially in contexts where privacy and data security are paramount. However, creating synthetic data requires carefully balancing utility—ensuring the data remains useful—with privacy, aimed at safeguarding sensitive information from exposure. In this talk, I will delve into these two key aspects of synthetic data and illustrate them through an auto insurance example. Additionally, I will share insights from my industry experience as the CEO of a synthetic data startup.





## Guidelines for Using Pseudonymization for Unstructured Data in South Korea



Hyun Joon Kwon

Former Director, Personal Data Secure Usage Division,  
Korea Internet & Security Agency, Republic of Korea



### BIOGRAPHY



Hyun-Joon Kwon has been involved in Personal Data Protection Policy Development and related governmental programs since 2011. He held the posts of Division Head, Director, etc. of Personal Data Protection Division in KISA. During his service of 24 years at KISA, he has been actively associated with internet policies regarding personal data protection, information security, Internet addresses, Internet governance, cloud computing, digital heritage preservation, and digital divide issues. He has actively participated in GPA(ICDPPC), APPA, WSIS, ICANN, APNIC, APEC ECSG, etc.



# Guidelines for pseudonymization of unstructured data in Korea



Hyun Joon Kwon, KISA

2024. 10.

## CONTENTS



1. Introduction
2. **Basics** of pseudonymization of unstructured data
3. Pseudonymization **Scenario** for unstructured data
4. Pseudonymization **Steps** for unstructured data

## 1.Intro

- ☑ The development of AI → **the demand for data utilization** from traditional structured data(table) to **unstructured data (images, videos, voices, texts)**.

\*\* Unstructured data such as images, videos, voices, and texts account for up to 90% of global data (IDC, '23)

### >> Difference between structured and unstructured data

#### | Structured Data |

(Def.) data that has a standardized format for efficient access by software and humans alike.

※ ex) Data in table format stored in columns and rows

- **Data processing methods and pseudonymization technologies are relatively simple.**

#### | Unstructured Data |

(Def.) data that doesn't follow conventional data models, in many different forms.

※ ex) Photos, videos, voice calls, conversation records, etc.

- Depending on the research purpose and context, data processing methods and **pseudonymization technologies are complex and diverse.**

2

## 1. Intro

- ☑ Unstructured data can also be used for **archiving purposes in the public interest, statistical purposes** or **scientific purposes**(ex AI research) **without the consent of the data subject** through pseudonymization special provisions (PDPA Art.28-2)

### >> Examples of pseudonymization of unstructured data

Images and Videos

- **MRI, CT, and X-ray images and videos** are used as learning data after pseudonymization for **medical AI research and development to diagnose (assist) specific diseases.**
- **Public CCTV footage** are used after pseudonymization for **developing an intelligent CCTV that detects and reports illegal activities.**

Voice and Texts

- **For developing a voice-generating AI for customer service, voice recording** of customer complaints consultation and response and **consultation record** information of public institutions are used as learning data after pseudonymization.

3

## 2. Basics of pseudonymization of unstructured data

1

**Comprehensively consider the purpose, context, and sensitivity** of data processing **to determine the information at risk of identification**

**and set a reasonable processing method and level.**

※ Refer to the checklist for identification risk of unstructured data [‘Guidelines for pseudonymized data’(2024. 2.) p. 52] and the risk mitigation action guide (p. 55).

- Minimizing data damage within the research purpose with the application of various security measures
  - To leave **data essential to the research purpose**, and
  - To **increase the level of pseudonymization** for **other data** or **supplement sufficient security measures** such as restrictions on bringing in other data and SW.

4

## 2. Basics of pseudonymization of unstructured data

2

**Risks should be thoroughly reviewed** and **appropriate security measures** should be implemented **from the preparatory stage** (from planning stage of research & technology development).

- Recommendation on Pseudonymization Technologies
  - ① Create and store **evidence** to confirm **the appropriateness and reliability** of pseudonymization technology.
  - ② After applying the pseudonymization technology, conduct **your own review of the processing results**.
  - ③ **In the stage of reviewing the appropriateness of pseudonymization**, checks including ① and ② (It is desirable that more than half of the review committee members be external experts.)
- Need to **strengthen internal control** of institutions using pseudonymized data.
- Minimize subsequent risks by **prompt deletion of pseudonymized data** after achieving the purpose of processing the pseudonymized data.

5

## 2. Basics of pseudonymization of unstructured data

3

When using pseudonymized unstructured data, establish **control measures** such as **restricting** access to and use of systems and SW related to **data restoration technology**.

\* Separate storage of additional information that can be used for data recovery, restriction of access to the recovery SW, etc.

- Even in the stage of providing AI services, we **continuously monitor** the possibility of infringement on the rights of data subjects, such as personal identification risks.
  - It is **impossible to completely eliminate** various risks that may arise in AI development and utilization situations **in advance**.

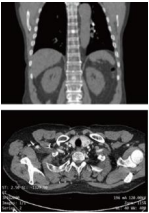
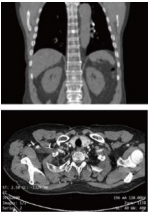
6

## 3. Pseudonymization **scenario** for unstructured data

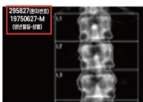
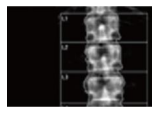


### (CASE 1) Development of AI medical diagnosis for breast cancer and bone density loss

A case of using **CT images (videos/images)** and **pathology records (text)** of breast cancer patients held by a university hospital **for internal research to develop AI diagnosis** for breast cancer and bone density loss by pseudonymizing them.

Since the processing environment is **securely controlled**, including restriction of recovery SW, and there is **no risk of identification**, **CT images can be used as is without pseudonymization**.

< Chest CT image >	Risk assessment	<ul style="list-style-type: none"> <li>- Chest CT image alone has little risk of identification</li> <li>- CT images taken 200 times per person can be used to restore the body shape using 3D reconstruction technology, etc.</li> <li>- Unique appearance and scars could lead to identification.</li> <li>- <b>The cloud-based closed research environment strictly controls the import of unauthorized data and programs</b>, making it impossible to apply 3D reconstruction technology.</li> </ul>	(Use as is)
	Data Processing	⇒ <b>The risk of identification</b> through 3D reconstruction is <b>unlikely to occur due to environmental controls</b> , so it can be <b>used as is without pseudonymization</b> .	


### 3. Pseudonymization scenario for unstructured data

Remove identifiable metadata from images and use it			
< Patient info in CT images > 	Risk Assessment	- Patient information in the image may pose a risk of personal identification if combined with other information' - Patient info(Patient number, date of birth, gender) is not necessary for the study.	<Black masking> 
	Data Processing	⇒ Deletion of patient info through black masking techniques	
Convert unstructured text data into structured data format and use it			
< Pathology record text > 	Risk Assessment	- Cancer pathology records contain a variety of unrefined, personally identifiable information that is unnecessary for research, which poses a risk of personal identification.	<converting to structured data> 
	Data Processing	⇒ Convert to structured data using Natural Language Processing(NLP) technology ⇒ Pseudonymization, If there is data that has a risk of identification ⇒ Due to the imperfection of pseudonymization technology, additional full-scale inspection is required.	

### 3. Pseudonymization scenario for unstructured data

#### (CASE 2) Development of AI medical diagnosis for oral diseases

University hospitals provide pseudonymized oral health check-up photos (images) to companies to develop AI medical diagnosis for oral diseases such as cavities and periodontitis


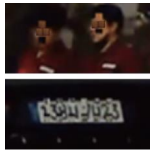
Blur unnecessary areas for research purposes and delete metadata for use			
< Teeth photo > 	Risk Assessment	- Almost no risk of identification of the teeth photo itself - No need for research on areas other than cavities - Metadata (name, age, etc.) in the oral photo poses a risk of identification	<Cavity part: Use as is> (Other: Blurring)
	Data Processing	⇒ The cavity area required for research is used as is, and the area unnecessary for research is blurred ※ The blurring level is set by the current level of restoration technology and data processing environment (ex. accessibility to other information) ⇒ Delete metadata unnecessary for research	

### 3. Pseudonymization scenario for unstructured data

#### (CASE 3) Development of AI for abnormal situation recognition in self-driving cars

After pseudonymizing the video footage of road conditions, it is provided to develop AI that recognizes **abnormal situations\*** in self-driving cars.

\* A person jumping into the road, another car suddenly cutting in front, jaywalking, etc.

Mask out unnecessary areas for research			
< Face/license plate image >  	Risk Assessment	- There is a risk of personal identification <b>when a person's face is clearly visible, or when a vehicle license plate is exposed so that the vehicle occupants can be inferred.</b> - For research purposes, <b>only the overall shape and movement of people and vehicles</b> are required.	< Masking >  
	Data Processing	⇒ <b>Masking of the face and license plate to an unidentifiable level</b>	



10

### 3. Pseudonymization scenario for unstructured data



#### (CASE 4) Development of AI chatbot capable of Korean conversation

Text data from **everyday conversations** between chat app users is pseudonymized and used for development of AI chatbots capable of Korean conversation.

Strictly filter and remove identifiable risk items and delete metadata for use

< conversation text file >  	Risk Assessment	- <b>Daily conversation data (text) contains a significant amount of personal data</b> , including private information.	< delete metadata, filter personal data >  
	Data Processing	⇒ <b>Replace metadata (user ID) with a random ID</b> to remove any connection to a specific individual. ⇒ Filter out (replace, delete) personal data	

Preventing pseudonymized data used in learning from being directly displayed in AI chatbot responses

< risk in chatbot responses >  	Risk Assessment	- If <b>pseudonymized data</b> used for learning is <b>not properly processed</b> and is used as a response from an AI chatbot, there is a <b>high risk of identification.</b>	Separation of learning DB from response DB  
	Data Processing	⇒ <b>Separate the 'learning DB' from the 'response DB'</b> to prevent sentences used in learning from being directly displayed in the responses. * Thoroughly check the identification risk of the response database.	

11



### 3. Pseudonymization scenario for unstructured data

#### (CASE 5) Development of AI training scenarios for call center staffs

Use pseudonymized voice data of customer service to develop AI training scenarios for call center staffs.

Convert voice data into text (STT, Speech To Text) and then use it after pseudonymization.

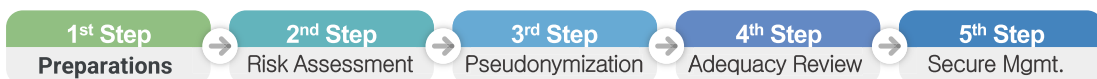
<p>&lt; Voice file &gt;</p> <p>목소리 개인식별정보</p>	Risk Assessment	<ul style="list-style-type: none"> <li>- Voice files contain <b>actual voice data (voice, tone, intonation, pronunciation, etc.)</b> of customers and employees, and <b>various personal data</b> exists in unrefined form in the conversation content.</li> <li>- In developing AI scenario for consultation, <b>it is important to understand the flow of questions &amp; responses and conversation according to the purpose of the consultation and customer characteristics, and the actual voice itself is not necessary.</b></li> </ul>	(① Convert to Text)
	Data Processing	<ul style="list-style-type: none"> <li>⇒ After converting to text by speech-to-text (STT) technology, pseudonymization(replacing/Deleting) is applied.</li> <li>⇒ Due to the imperfection of pseudonymization technology, <b>additional full-scale inspection is required</b></li> </ul>	(② Replacing/Deleting personal data)

12

### 4. Pseudonymization Steps for unstructured data

Regarding the pseudonymization of unstructured data, it is recommended to follow the same pseudonymization process step-by-step in Chapter 2 of the "Guidelines for Pseudonymized data" but additionally to consider and implement safety measures that reflect the special nature of unstructured data.

#### Step-by-step procedure for pseudonymization



- 1 Preparations \* The stage of **setting and reviewing the purpose** of pseudonymization and **selecting the target** that fits the purpose
  - Clarify the type and scope of data required **to achieve the purpose in unstructured data**, **derive** personal data, and **select the target for pseudonymization**
- 2 Risk Assessment \* Stage of reviewing the risk of pseudonymization **to determine the method and level of pseudonymization**
  - After **comprehensively reviewing the identification risk** from the '**data itself**' and the '**processing context**', the method and level of pseudonymization are determined.
  - Review whether there is ① identification information, ② identifiable information, ③ **unique information**, and ④ information that has a significant impact on the information subject after re-identification

13

## 4. Pseudonymization Steps for unstructured data

### 3 Pseudonymization ※ Pseudonymization steps based on risk assessment results and item-by-item pseudonymization plan

- Distinguish between items that do not require pseudonymization and those that require pseudonymization
- Information that is necessary to achieve the purpose of processing **but has a low risk of personal identification** may be **used as is** without pseudonymization.
- Information that is necessary to achieve the purpose of processing **and has a high risk of personal identification** must be **used in pseudonymized form**.

### 4 Adequacy Review ※ The adequacy review committee, **including external experts**, reviews the **appropriateness of the processing purpose, risks, pseudonymization, and the possibility of achieving the purpose, etc.**

- whether pseudonymization was performed in a reasonable manner and at a reasonable level, **taking into account the characteristics of the unstructured data and the purpose and environment of processing**.
- **the appropriateness and reliability of the technology** used to pseudonymize unstructured data,
- whether additional inspections have been conducted **to sufficiently reduce residual risks** due to limitations of the technology.
- Ensuring **objectivity and expertise** by having **more than half of the members be external experts**

14

## 4. Pseudonymization Steps for unstructured data

### 5 Secure Management ※ **The stage of monitoring and managing the possibility of re-identification, etc.** in the process of utilizing pseudonymized data

- **Security measures** are necessary for various risks that may occur **after pseudonymization**
- The level of implementation of post-management is judged based on **the degree of effort to minimize residual risk**.
- In particular, **continuous monitoring** of the possibility of infringement of the rights of the data subject is important **during the operation of AI-based services**.
- **Immediate Risk mitigation measures** such as stopping the processing of the relevant pseudonymized data **upon discovery of a risk** are necessary.

15



