行政院所屬各機關因公出國報告書

（出國類別：開會）

出席第 47 屆全球隱私大會
(Global Privacy Assembly, GPA)
出國報告

出國人員服務機關	職稱	姓名
個人資料保護委員會籌備處	專員	何慕凡
個人資料保護委員會籌備處	視察	林威廷
個人資料保護委員會籌備處	專員	游蕙瑜
個人資料保護委員會籌備處	設計師	曾志翔

會議國家：韓國

出國期間：民國114年9月14日至114年9月18日

報告日期：民國114年11月

出席第 47 屆全球隱私大會(Global Privacy Assembly, GPA)

目錄

壹、背景說明及會議摘要

本屆全球隱私大會（Global Privacy Assembly, GPA）為全球隱私與資料保護領域的旗艦論壇，目前共有來自英國、美國、加拿大、日本、歐盟、香港、紐西蘭、澳洲、阿根廷、比利時、巴西、智利、法國、德國、澤西、墨西哥、南韓等95國，共148個超國家級（supranational authorities）、國家級（national authorities）、次國家級（sub-national authorities）個人資料保護機構之正式會員；並有包含世界銀行（World Bank）、歐洲委員會（European Commission）、歐洲理事會（Council of Europe）等在內的40個國際與非國際組織觀察員共同參與[1]。

第47屆GPA會議業於2025年9月15日至9月19日於韓國首爾辦理，主題為「AI在日常生活中的運用：資料與隱私議題」（*Artificial Intelligence in Our Daily Lives: Data and Privacy Issues*），由韓國個人資料保護委員會（Personal Information Protection Commission, PIPC）主辦。

本次會議為期五日，議程規劃如下：首日（9月15日）為會前活動，包含公司實地考察、文化交流及歡迎會；次二日（9月16日至9月17日）為公開議程，由主辦方邀請來自產官學研等各界隱私及個人資料保護專家，透過主題演講、專題座談、爐邊談話與平行論壇，針對人工智慧與隱私保護相關議題進行交流分享，討論內容包括「以信任為基礎的全球資料治理與AI生態系（Global Data Governance for a Trust-Based AI Ecosystem and Community）」、「去識別化資料應用（Expanding the Use of Pseudonymized Data）」、「合成資料實務（Synthetic Data in Practice）」、「AI訓練資料的法律依據（Legal Bases for Processing Training Dataset

[1] GPA正式會員名單，詳參官網：https://globalprivacyassembly.com/participation-in-the-assembly/list-of-accredited-members/

s for AI）」、「醫療保健服務與AI（Health Care Services and AI）」、「個資保護機構的角色（DPAs' Establishment and Role）」、「AI時代的資料保護法修正（Rethinking and Amending Data Protection Law in the Age of AI）」、「AI智能代理與隱私影響（AI Agents and Privacy Implications）」、「支持AI創新機制（Mechanisms for Supporting Innovation in AI）」、「跨境資料傳輸互通性（Expanding Interoperability in Cross-Border Data Transfer）」、「情感AI與隱私（Emotional AI and Privacy）」、「醫療資料再利用（Re-using Health Data: Balancing AI Health Innovation and Privacy in a Cross-Border Context）」及「資料保護救濟與互通性（Redress and Interoperability of Data Protection: the Consumer Perspective）」，並於9月17日晚間辦理 GPA 頒獎及閉幕晚宴。末二日（9月18日至9月19日）則為正式會員及觀察員限定之閉門會議，主要就大會事務進行討論。除主辦方 PIPC 籌劃之正式活動外，會場同樣開放會員及觀察員辦理聚焦特定議題之公開或非公開場邊會議，以促進多方交流與合作。

會後，共有20個個資監管機構共同簽署一份AI創新隱私聯合聲明[2]。此聲明由韓國個人資料保護委員會（PIPC）發起，最初參與者包括法國、英國、愛爾蘭及澳洲，後續擴展至加拿大、德國、義大利等，共計20國。聲明將致力於倡導對人工智慧應用進行可信賴的監管，同時兼顧創新友善性和永續的資料保護保障。此舉不僅擴大了韓國在創新友善AI政策方面的國際共識，也強調了個資監管機構在AI時代應扮演更積極主動的角色。

[2] 相關新聞請參考：https://www.pipc.go.kr/np/cop/bbs/selectBoardArticle.do?bbsId=BS074&mCode=C020010000&nttId=11511

韓國個人資料保護委員會主席高學秀（Haksoo Ko）開場(含南韓總統李在明表示歡迎詞)

韓國個人資料保護委員會主席高學秀（Haksoo Ko）開場

貳、會議日程表

日期	時間	行程
9/15 (一)	13:00 ｜ 16:30	參訪三星創新博物館 Samsung Innovation Museum Tour
9/16 (二)	09:00 ｜ 09:10	開場致歡迎詞 韓國個人資料保護委員會主席Haksoo Ko（Chairman, Personal Information Protection Commission, Republic of Korea）
	09:10 ｜ 09:40	主題演講一/Keynote 1 Signal 基金會總裁Meredith Whittaker（President, Signal Foundation）
	場次一：AI 時代的全球資料治理 Session 1: Global Data Governance in the AI Era	
	09:40 ｜ 10:40	主持人：韓國個人資料保護委員會主席Haksoo Ko 與談人： 英國資訊委員辦公室資訊專員John Edwards（Information Commissioner, ICO, UK） 法國國家資訊自由委員會主席Marie-Laure Denis（ President, CNIL, France） 新加坡國立大學教授Simon Chesterman（Professor, National University of Singapore） 哈佛創新實驗室代表、前美國聯邦貿易委員會委員暨前微軟公司副總裁Julie Brill（Harvard Innovation Lab; Former FTC Commissioner; Former Microsoft Executive）

日期	時間	行程
	場次二：透過去識別化個人資料以促進創新 Session 2: Pseudonymization of Personal Data to Facilitate Innovation	
	11:10 ｜ 12:00	主持人：國際隱私專業人員協會研究與洞察部總監Joe Jones（Research & Insights Director, International Association of Privacy Professionals） 與談人： 新加坡個人資料保護委員會政策與技術總監Adeline Tung（Director of Policy & Technology, PDPC,Singapore） 英國資訊專員辦公室主任Chris Taylor（Director, ICO, UK） 歐洲資料保護委員會秘書處主任Isabelle Vereecken（Head of the Secretariat, EDPB） 印度電子與資訊科技部科學官Vikash Chourasia（Scientist D, Ministry of Electronics and Information Technology, India）
	場次三：獨立合成資料的實務應用：機會與挑戰 Session 3: Synthetic Data in Practice: Opportunities and Challenges	
	12:00 ｜ 12:40	主持人暨發表人：加拿大渥太華大學醫療人工智慧研究講座教授Khaled El Emam（Canada Research Chair, Medical AI at the University of Ottawa） 與談人： 韓國首爾大學教授Sungkyu Jung（Professor, Seoul National University） 德國 CARIAD 公司副總裁Marc Holzäpfel（Vice President, CARIAD）

日期	時間	行程
	爐邊對談：人工智慧對醫療服務與隱私的影響 Fireside Chat: Impact of AI on Healthcare Services and Privacy	
	14:10 | 14:50	主持人：梨花女子大學教授Ho Bae（Ewha Womans University, 韓國首爾） 與談人： 以色列本·古里安大學公共衛生教授Ran Balicer（Public Health Professor, Ben Gurion University） Kakao Healthcare公司首席研究官Sooyong Shin（Chief Research Officer, Kakao Healthcare）
	14:50 | 15:00	主題演講二/Keynote 2 歐盟民主、司法、法治與消費者保護專員Michael McGrath（Commissioner for Democracy, Justice, the Rule of Law, and Consumer Protection, EU）
	場次四：為人工智慧目的處理個人資料的合法性 Session 4: Lawfulness of Processing Personal Data for Purposes of AI	
	15:20 | 16:20	主持人：Hunton Andrews Kurth LLP 律師事務所資訊政策領導中心主席Bojana Bellamy（President of Hunton Andrews Kurth LLP’s Centre for Information Policy Leadership, CIPL） 與談人： 歐洲資料保護委員會主席Anu Talus（Chair, EDPB） 阿根廷個人資料保護局局長Beatriz Anchoreña（Commissioner, AAIP, Argentina） 愛爾蘭資料保護委員會委員Dale Sunderland（Commissioner, DPC, Ireland）

日期	時間	行程
		韓國科學技術院教授Byoung Pil Kim（Professor, KAIST）
	平行論壇1-A：新興設立與制度化資料保護機構（由APPA主導） Parallel Session 1-A : Newly Establishing and Institutionalizing DPAs (led by the APPA)	
	16:30 ｜ 17:30	主持人：新加坡個人資料保護委員會副主席Denise Wong（Deputy Commissioner, PDPC, Singapore） 與談人： 韓國個人資訊保護委員會副主席Janghyuk Choi（Vice Chairperson, PIPC, Korea） 紐西蘭隱私專員辦公室隱私專員Michael Webster（Privacy Commissioner, OPC, New Zealand） 南非資料保護委員會委員Pansy Tlakula（Chairperson, IRSA, South Africa） 世界銀行代表Taylor Reynolds（Practice Manager, World Bank）
	平行論壇1-B：10 年資料保護：承先啟後，邁向人工智慧時代人道行動的未來挑戰（由 WG AID 與 ICRC 主導） Parallel Session 1-B: （10 years of Data Protection in Humanitarian Action: Building on the past to navigate future challenges for Humanitarian Action in the age of AI (led by the WG AID and the ICRC)）	
	16:30 ｜ 17:30	主持人： 國際紅十字會資料保護辦公室主任Massimo Marelli （Head, Data Protection Office at ICRC） 瑞士聯邦資料保護與資訊專員國際事務與法語事務代表Catherine Lennman（Delegate for International Affairs and Francophonie, FDPIC）

日期	時間	行程
		與談人： 阿根廷個人資料保護局委員Beatriz Anchorena（Commissioner, AAIP, Argentina） 聯合國世界糧食計劃署全球隱私辦公室主任兼資料保護長Carmen Casado（DPO and Director of the Global Privacy Office, UN World Food Programme） 韓國個人資料保護委員會資深副主席Youngsu Jong（Senior Deputy Director, PIPC, Korea） 肯亞資料保護委員辦公室Immaculate Kassait（Data Commissioner, ODPC, Kenya） 日本中央大學政策研究學部副教授Hiroshi Miyashita（Associate Professor, Faculty of Policy Studies at Chuo University） 荷蘭馬斯垂克大學歐洲隱私與網路安全中心主任Cosimo Monda（Director of the Maastricht European Centre on Privacy and Cybersecurity, Maastricht University） 國際紅十字會與紅新月會國際聯合會法務主管兼隱私保護辦公室負責人James De France（Managing Legal Counsel and Head of the Data Protection Office, IFRC） 聯合國難民署資料保護與隱私事務主任Alex Novikau（Chief Data Protection and Privacy Officer, UNHCR） 歐洲資料保護監督機關專員Wojciech Wiewiórowski（European Data Protection Supervisor, EDPS）
	平行論壇1-C：在人工智慧時代重新思考資料保護法（由隱私權未來論壇FPF主導） Parallel Session 1-C：Rethinking Data Protection Law in the Age of AI（led by the FPF）	
	16:30	主持人：隱私未來論壇副總裁Gabriela Zanfir-Fortuna

日期	時間	行程
	| 17:30	（Vice President, Future of Privacy Forum） 與談人： 澳洲資訊專員辦公室委員Carly Kind（Commissioner, OAIC, Australia） 丹麥哥本哈根大學教授Christopher Kuner（Professor, Copenhagen University） 韓國首爾大學教授Sangchul Park（Professor, Seoul National University） Prosus集團首席隱私長Monika Tomczak-Górlikowska （Chief Privacy Officer, Prosus Group）
9/17 （三）	09:00 | 09:30	主題演講三/Keynote 3 普林斯頓大學教授D. Graham Burnett（Professor, Princeton University）
	場次五：代理式人工智慧與隱私 Session 5: Agentic AI and Privacy	
	09:30 | 10:30	主持人：韓國首爾大學教授Yong Lim（Professor, Seoul National University） 與談人： 英國資訊委員辦公室John Edwards（Information Commissioner, ICO, UK） 隱私未來論壇執行長Jules Polonetsky（Chief Executive Officer, Future of Privacy Forum） Google 全球隱私、安全與保障總監Kate Charlet（Global Director for Privacy, Safety, and Security, Google LLC）

日期	時間	行程
		LG AI 研究中心策略部主管Yoochul Kim（Head of Strategy Unit, LG AI Research）
	場次六：支持人工智慧創新的機制與政策工具 Session 6: Mechanisms and Policy Instruments to Support AI Innovation	
	11:00 ｜ 12:00	主持人：國際隱私專業人員協會總裁兼執行長J. Trevor Hughes（CEO, International Association of Privacy Professionals） 與談人： 法國國家資訊自由委員會國際事務專員Bertrand du Marais（International Affairs Commissioner, CNIL, France） 愛爾蘭資料保護委員會主席Des Hogan（Chairperson, DPC, Ireland） Kakao 首席隱私長Yeonjea Kim（Chief Privacy Officer, Kakao） Meta 公司副總裁Stefano Fratta（Vice President, Meta）
	13:30 ｜ 13:50	主題演講四/Keynote 4 OpenAI 首席策略長Jason Kwon（CSO, OpenAI）
	場次七：促進跨境資料傳輸的互通性 Session 7: Enhancing Interoperability in Cross-Border Data Transfers	

日期	時間	行程
	13:50 | 14:50	主持人：加拿大英屬哥倫比亞省資訊及隱私專員Philippe Dufresne（Privacy Commissioner, Commissioner, OIPC, BC Canada） 與談人： 丹麥哥本哈根大學教授Christopher Kuner（Professor, University of Copenhagen） 美國大學教授Alex Joel（Professor, American University） 肯亞資料保護委員辦公室Immaculate Kassait（Data Commissioner, ODPC, Kenya） 日本個人資料保護委員會委員Yuji Asai（Commissioner, PPC, Japan）
	平行論壇2-A：青少年隱私：實務操作 Parallel Session 2-A :Youth Privacy: Mechanics	
	15:10 | 16:10	主持人：加拿大英屬哥倫比亞省資訊及隱私專員Michael Harvey（Commissioner, OIPC, BC Canada） 致詞：美國聯邦貿易委員會專員Melissa Holyoak（Commissioner, FTC, USA） 與談人： 韓國個人資料保護委員會委員Sanghee Park（Commissioner, PIPC, Korea） 5Rights 基金會執行董事Leanda Barrington-Leach（Executive Director, 5rights） TikTok 歐洲區隱私負責人Elaine Fox（Head of Privacy, Europe, TikTok） Apple 公司全球隱私與線上安全主管Hilary Ware（Head of Privacy Legal and Online Safety, Apple）

日期	時間	行程
	平行論壇2-B：資料保護的救濟與互通性：消費者觀點（由亞太數位消費者對話主導） Parallel Session 2-B :Redress and Interoperability of Data Protection: The Consumer Perspective (led by the Asia Pacific Digital Consumer Dialogue)	
	15:10 ｜ 16:10	主持人： 日本消費者組織代表Amy Kato（Consumers Japan） 與談人： 義大利資料保護局董事會Guido Scorza（Board Member, Garante, Italy） 中央大學教授Hiroshi Miyashita（Professor, Chuo University） 亞太數位消費者對話顧問Javier Ruiz Diaz（Advisor, Asia-Pacific Digital Consumer Dialogue） Hunton Andrews Kurth LLP 律師事務所總監Natascha Gerlach（Director, CIPL） 韓國進步網路 Jinbonet 總裁ByoungIl Oh（President, Korean Progressive Network Jinbonet）
	平行論壇3-A：健康資料再利用：在跨境背景下平衡人工智慧健康創新與隱私（由 OECD 主導） Re-Using Health Data: Balancing AI Health Innovation and Privacy in a Cross-Border Context (led by the OECD)	
	16:20 ｜ 18:00	開幕致詞暨主持人： 經濟合作暨發展組織資料流通、治理與隱私處處長Clarisse Girot（Head of Division for Data Flows, Governance and Privacy, OECD） 主持人：

日期	時間	行程
		經濟合作暨發展組織隱私、資料治理與數位安全政策分析師Limor Shmerling Magazanik（Policy Analyst, Privacy, Data Governance and Digital Security, OECD） 主題演講： 加拿大渥太華大學醫學人工智慧加拿大研究講座教授Khaled El Emam（Canada Research Chair, Medical AI at the University of Ottawa） 與談人： 諾華醫療有限公司亞太區、中東非洲及全球健康資料隱私、數位與人工智慧主管Nitin Dhavate（Head of Data Privacy, Digital & AI (DPDAI), Asia Pacific, MEA & Global Health, Novartis Healthcare Pvt. Ltd.） 韓國首爾峨山醫院研究副教授Soyoung Yoo（Research Associate Professor, Asan Medical Center） Kakao Healthcare 首席研究官Sooyong Shin（Chief Research Officer, Kakao Healthcare） 愛爾蘭資料保護委員會副專員Gráinne Hawkes（Deputy Commissioner, DPC, Ireland） 澳洲墨爾本大學法學院教授Mark J Taylor（Professor, Melbourne Law School） 加拿大英屬哥倫比亞省資訊及隱私專員Michael Harvey（Commissioner, OIPC, BC Canada）閉幕致詞： 韓國個人資料保護委員會政策局局長Cheongsam Yang（Director-General, Head of the Personal Information Policy Bureau, PIPC, Korea） 參考文件：促進跨境為公共利益目的的健康資料二次利用 | OECD（Facilitating the secondary use of health data for public interest purposes across borders | OECD）

日期	時間	行程
	平行論壇3-B：教育科技的資料治理：如何保護兒童隱私？ （由數位經濟工作小組DEWG與聯合國兒童基金會UNICEF主導） Parallel Session 3-B : Data Governance for EdTech: How to protect children’s Privacy? (led by the DEWG and the UNICEF)	
	16:20 ｜ 18:00	主持人： 法國國家資訊自由委員會國際事務專員Bertrand du Marais（International Affairs Commissioner , CNIL, France） 聯合國兒童基金會前瞻與政策處主任Jasmina Byrne （Chief of Foresight and Policy, UNICEF） 與談人： 韓國首爾大學教授JongYoun Rha（Professor, Seoul National University） 法國國家資訊與自由委員會法務專員Zeida Gerard-Besset（Legal officer, CNIL, France） 加拿大安大略省資訊與隱私專員辦公室專員Patricia Kosseim（Commissioner, IPC, Ontario Canada） 菲律賓隱私專員辦公室組長Ivy Grace T.Villasoto（Division Chief, NPC, Philippines） 微軟首席隱私長Cari Benn（Chief Privacy Officer, Microsoft）
	18:30 ｜ 21:30	GPA獎項頒發與晚宴

參、會議情形

一、各場次重點

主題演講一（Keynote 1）

Signal 基金會總裁梅瑞迪絲・惠特克（Meredith Whittaker，President, Signal Foundation）演講

本場主題演講由Signal基金會（Signal Foundation）總裁Meredith Whittaker主講，其為一位AI倫理專家、隱私倡議者和前Google工程師，著重於AI監控風險和推動科技勞工權益等議題[3]。

（一）歷史教訓：W總裁將重點放在重新審視過去的歷史。她認為，在1990年代將加密技術的自由化當作隱私權的勝利是嚴重的失誤。當時美國政府希望在享受商業網際網路帶來的經濟利益的同時，保留透過

[3] Whittaker, M. (n.d.). Meredith Whittaker. In Wikipedia. Retrieved September 20, 2025, from https://en.wikipedia.org/wiki/Meredith_Whittaker

加密後門(backdoors)進行監控的能力，最終，雖然加密技術得以自由化，但她認為隱私權並沒有真的獲勝；實際上，這個結果促成了以監控式廣告(surveillance advertising)為基礎的商業模式，使科技巨頭有強烈的經濟誘因去大規模蒐集個人資料。因此，雖然強加密技術存在，但它主要被用來保護商業利益，而非一般人的隱私，這導致了隱私名義上被重視、實際上卻不然的矛盾情況。

（二）當前隱私議題：

W總裁認為當前隱私面臨的威脅議題，一方面來自立法層面的直接攻擊，亦即各國政府（如英國、歐盟）持續推動法案[4]，要求在端到端加密系統中植入後門(backdoors)，她認為，這種要求是無視技術現實、天馬行空的想法(magical thinking)。

另一方面的威脅議題則來自作業系統，並且是AI發展過程中所產生的風險。講者說明，作業系統（如iOS, Android, Windows）正在從中立平台轉變為整合AI代理人（AI Agent）的主動角色。這些AI代理人為了提供所謂的便利，被授予了存取設備上所有應用程式資料的權限。這種架構上的改變，使得應用程式自身（如Signal）所做的隱私保護措施可能被繞過，其危險性與根本性遠超以往。其舉例說明，微軟Recall功能[5]和蘋果Siri對第三方應用程式資料的存取，都是具體存在的風險。

[4] 例如，英國的《調查權力法（Investigatory Powers Act)》和歐盟的 CSAR（或稱聊天控制法案, chat control legislation)。這些法案持續要求建立只允許「好人」使用的後門。

[5] 微軟Recall是Windows 11 Copilot+ PC的AI功能，能透過自然語言搜尋或時間線檢索過去電腦畫面內容，包括應用程式、文件和網站，並直接跳回該處繼續操作。Microsoft. (2025, August 28). Privacy and control over your Recall experience. https://support.microsoft.com/en-us/windows/privacy-and-control-over-your-recall-experience-d404f672-7647-41e5-886c-a3c59680af15

（三）具體行動呼籲

面對前述議題，W總裁呼籲採取更全面的策略。她強調，持續捍衛加密技術、反對後門是必要的基礎；不過，更重要的是必須主動應對來自作業系統層級的威脅。她提出的具體行動包括：首先，要求開發者層級的選擇退出權(Developer-level opt-outs)，應用程式開發者應有權利選擇退出作業系統層級的AI資料掃描與存取，以確保其應用程式內的隱私承諾不被破壞。其次，要求徹底的透明度(Radical transparency)，作業系統供應商必須清楚、公開地說明其AI系統存取、收集、處理和傳輸了哪些數據，讓外界得以監督。

場次一（Panel Session 1）：AI 時代的全球資料治理（Global Data Governance in the AI Era）

主持人及現場與談嘉賓，由左至右分別為Haksoo Ko、John Edwards、Marie-Laure Denis、Simon Chesterman、Julie Brill。

主持人：Haksoo Ko（韓國個人資料保護委員會主席，Chairperson, PIPC, Korea）

與談人：

- John Edwards（英國資訊委員辦公室辦公室資訊專員，Information Commissioner, ICO, UK）
- Marie-Laure Denis（法國國家資訊與自由委員會主席，President, CNIL, France）

- Simon Chesterman（新加坡國立大學院長，Dean, National University of Singapore）
- Julie Brill（哈佛創新實驗室代表、前美國聯邦貿易委員會委員暨前微軟公司副總裁，Harvard Innovation Lab; Former FTC Commissioner; Former Microsoft Executive）

本場會議議題以 AI 時代下全球資料治理的困境與前景為主軸，與談者從不同角度剖析了其中的矛盾、權衡與可能的解決路徑，主要可歸納為以下三大主題。

（一）全球創新與在地監管的根本矛盾：

座談的核心始於韓國 K主席所指出的矛盾：AI 模型依賴全球資料來訓練，而資料法規則是地域性的。此觀點獲得與談者普遍認同。英國E 專員指出，對監管者而言，要以國內職權監管無國界的科技巨頭，是巨大的挑戰。新加坡C 院長認為，這可引申為「規則制定者」與「規則接受者」之間的權力不對等。許多國家因害怕錯失經濟發展機會（FOMO），而在監管上處於被動地位，傾向採取較寬鬆的標準。這凸顯了在全球化的數位經濟中，各國在維護主權、保護公民與擁抱創新之間所面臨的難題。

（二）監管框架的權衡：在「創新促進」與「權利保障」之間尋找平衡：

如何平衡創新與監管，是本次討論的另一焦點。法國D 主席詳細闡述了歐盟模式係試圖透過《人工智慧法》等一系列立法，在 GDPR 的基礎上建立一個既能促進資料再利用，又能保障基本權利的框架。其目標是讓監管成為「可信賴 AI」的基石，而非絆腳石。此外，英

國E 專員所描述的英國則展現了更為「輕觸」與「放手」的趨向，例如在自動化決策上放寬限制，顯示出更側重於為創新掃除障礙的政策考量。不過，新加坡C 院長也提到，即使歐盟在某種程度上可能係以犧牲創新為代價來保護權利，說明此種權衡仍然困難。

（三）治理模式的演進：從既有法規的延伸到跨域合作的未來：

面對新興科技，與談者均同意既有的法律框架面臨巨大挑戰。多位與談者皆提到，將GDPR的「資料最小化」、「目的限制」等原則應用於需大量資料的AI模型時，會產生法律解釋上的困難。對此，許多監管機構正積極透過發布指引、推動隱私增強技術（Privacy-Enhancing Technologies, PETs），如聯邦式學習（Federated Learning）來應對。

就未來方向而言，治理模式需要更多積極合作，例如建立涵蓋政府、產業與公民社會的多方利害關係人全球對話平台；或在實務操作層面上，各國國內跨部門監管合作亦十分重要，因為資料保護機關已無法獨力應對AI帶來的競爭、安全與內容治理等多重議題。這意味著，未來的AI治理將不再是單一部門的職責，而是一個需要國內外、公私部門共同協作的複雜合作體系。

場次二（Panel Session 2）：透過去識別化個人資料以促進創新（Pseudonymization of Personal Data to Facilitate Innovation）

主持人及現場與談嘉賓，由左至右分別為Joe Jones、Adeline Tung、Chris Taylor、Isabelle Vereecken、Vikash Chourasia。

主持人：Joe Jones（國際隱私專業人員協會研究與洞察部總監，Director of Research and Insights, IAPP）

與談人：

- Adeline Tung（新加坡個人資料保護委員會政策與技術總監，Director of Policy & Technology, PDPC, Singapore）
- Chris Taylor（英國資訊委員辦公室主任，Director of International Regulatory Cooperation, ICO, UK）

- Isabelle Vereecken（歐洲資料保護委員會秘書處主任，Head of the Secretariat, EDPB）
- Vikash Chourasia（印度電子與資訊科技部科學官，Scientist D, Ministry of Electronics and Information Technology, India）

本場會議深入探討了「假名化（pseudonymization）」作為平衡資料創新與隱私保護的關鍵技術，匯集了歐洲、英國、新加坡與印度等不同司法管轄區的觀點與實踐。會議討論情形如下：

（一）新加坡經驗：監管實務與創新應用

新加坡T總監指出，新加坡《個人資料保護法》（PDPA）雖未明確定義「假名化」，但監管實務上已將其視為「去識別化」技術的重要組成部分。PDPC透過多項實務指引，如《實用技術指南：基礎匿名化（Practical Technical Guide on Basic Anonymization）》，提供系統化的五步驟流程，涵蓋紀錄抑制、字元遮罩、概括化與資料聚合等技術，協助企業安全處理資料。T總監強調，指引的目的不僅是提供技術範例，更在於幫助企業理解如何在保障隱私的前提下安全利用資料。

此外，T總監指出新加坡監理設計的兩大原則為「監管簡潔性（Regulatory Simplicity）」與「監管清晰性（Regulatory Clarity）」，即法規應簡單明確、具可操作性，並透過具體指導文件協助企業理解合規要求。近期PDPC發布《隱私增強技術採用指南（Privacy-Enhancing Technologies Adoption Guide）》草案，協助企業依據業務需求與風險情境選擇適當技術。

在實務層面，假名化被視為兼顧隱私與創新的可行途徑，可讓組織在不違背資料最小化原則下推動AI與數據分析應用。T主任進一步介紹PDPC自2022年推行的「監管沙盒（Regulatory Sandbox）」計畫，鼓勵企業測試包括假名化在內的多種隱私增強技術。代表性案例為Grab公司，其透過假名化分離可識別與非識別資料、設置權限區隔，並結合可信執行環境（TEE）確保運算安全。該案例顯示假名化可促進跨部門資料整合與治理能力提升。

最後，T總監指出推動假名化仍面臨技術複雜性、成本負擔與企業認知不足等挑戰。她強調國際合作的重要性，說明新加坡正與東協（ASEAN）、亞太隱私機構（APPA）及OECD合作推動區域指南與最佳實踐，建立跨境資料流通的信任基礎。

（二）英國經驗：法律明確化與實務落地

英國T主任表示，英國法律對假名化資料有明確定義，即資料若不與額外資訊結合即無法識別個人，而該額外資訊必須以適當技術與組織措施加以保護。英國資訊專員辦公室（ICO）已發布多份指南，說明假名化在資料保護法中的地位與操作方法，為產業提供明確行動依據。

在監理哲學上，英國強調假名化的核心價值在於平衡「資料實用性（data utility）」與「隱私保護」。與完全匿名化不同，假名化資料能保留更多可用資訊，允許進行跨資料集連結與長期追蹤分析，特別有助於AI模型訓練與公共政策研究。T主任指出，假名化使研究者得以觀察長期趨勢與稀有事件，兼顧精確性與隱私保護，實質上是一項兼具創新與合規的治理措施。

在跨境資料傳輸方面，假名化亦被視為「適當保障措施（appropriate safeguard）」。T主任強調，企業若能證明其在處理與傳輸中採用假名化與相關安全措施，不僅可降低風險，亦能增強國際合作信任，體現英國監管強調的「責任導向（accountability）」精神。

英國的實務案例包括公共衛生與研究領域：國民保健署（NHS）及研究機構建立「可信研究環境（TREs）」與「安全資料環境（SDEs）」以提供受控存取假名化資料。另一重點為ICO沙盒專案「我們的未來健康（Our Future Health）」，該專案以假名化機制蒐集大規模健康資料，確保研究透明與倫理合規，成為信任式資料治理的典範。

T主任亦坦言仍存在技術成本高與能力落差等挑戰。ICO 正啟動新研究以釐清假名化在 AI訓練中的角色與法律界定，期盼透過制度化框架建立更穩定的信任基礎。

（三）歐盟經驗：法律定義與情境性評估

法國V主任說明，《一般資料保護規則》（GDPR）已明確定義假名化，並於2025年1月由EDPB通過假名化指導意見，闡述其四項主要價值：

1.作為資料最小化與安全措施，可降低洩露風險；

2.符合「隱私始於設計（Privacy by Design）」原則，應自系統開發初期即納入考量；

3.可促進資料控制者在「合法利益（legitimate interest）」下的資料利用；

4.作為跨境資料傳輸的補充保障措施（supplementary measures）。

V主任同時介紹歐洲法院（CJEU）近期裁決[6]，採「相對性評估」原則，認定同一份假名化資料其屬性會依持有者而異：對資料控制者而言，若掌握關聯資訊則仍屬個資；對資料接收者而言，若無合理手段可識別個人，則可能不受GDPR約束。此判例為資料共享開啟彈性空間，但仍維持匿名化的高門檻。

在實務應用方面，V主任提及假名化已在歐盟健康數據空間（EU Health Data Space）、臨床試驗及交通移動領域中普遍採用，用以兼顧資料可用性與隱私保護。

（四）印度經驗：分層式監管與制度探索

印度C科學官介紹，印度於2023年通過《數位個人資料保護法》（DPDP2023），採原則導向的輕觸式監管（light-touch regulation），目前尚未正式施行，法律中亦未明確承認假名化作為法定技術措施。然而，他指出假名化在實務上具兩項重要價值：

一是作為建立用戶信任的措施，強化資料再利用（如 AI訓練）之正當性；二是作為額外的安全保護手段，兼顧風險緩解與商業效益。

[6] 在此判決中法院認為假名化（pseudonymised）資料的個人資料屬性需視情境評估，從接收者角度判斷是否具「合理可能手段」還原身分；對無合理方法還原身分的接收者而言，則可能被視為匿名（anonymous）資料。參European Data Protection Supervisor v. Single Resolution Board, C-413/23 P (Eur. Ct. Justice Sept. 4, 2025), https://curia.europa.eu/juris/document/document.jsf?text=&docid=303863&pageIndex=0&doclang=EN

C科學官進一步說明，印度正考慮採取「分層式監管」模式（sector-specific approach），由特定產業如金融與醫療率先制定假名化規範，再逐步推廣至其他領域。該模式旨在在風險可控的前提下探索多元實踐。

目前，政府主要聚焦於匿名化數據發布與AI公共計畫資料開放，而私營部門則逐步採用假名化作為內部風險緩解機制。未來重點包括發布官方技術指引、推動教育與認知提升，以及建立「監管沙盒」以鼓勵行業實驗。

本次與談展現了假名化在全球資料保護體系中的多元實踐。各國雖在法制成熟度與技術採納程度上存在差異，但共同目標均在於透過假名化技術實現「隱私保護與資料利用並行」的平衡。討論也凸顯國際協作的重要性，唯有透過跨境標準與概念的整合，方能建立可信賴的全球資料治理架構。

場次三（Panel Session 3）：獨立合成資料的實務應用：機會與挑戰（Synthetic Data in Practice: Opportunities and Challenges）

主持人與與談嘉賓：由左至右分別為Sungkyu Jung、Marc Holzäpfel、Khaled El Emam

主持人：Khaled El Emam（加拿大渥太華大學教授，Professor, University of Ottawa）

與談人：

- Sungkyu Jung（韓國首爾大學教授，Professor, Seoul National University）
- Marc Holzäpfel（德國CARIAD公司副總裁，Vice President, CARIAD）

本場座談聚焦於合成資料（Synthetic Data）在實務應用中的價值、風險與治理挑戰。與會者從學術、產業及監理三個角度，探討如何在促進創新與保障隱私之間取得平衡。整體討論圍繞三個主軸：

（一）合成資料的價值：兼顧創新應用與隱私保護

與會者一致肯定合成資料作為一種新興技術，其價值不僅限於隱私保護。E教授從學術角度闡述了合成資料在解決數據稀缺（如罕見疾病研究）與演算法公平性（如去偏誤）等問題上的巨大潛力。J教授則以韓國的實例，展示合成資料在公共服務（市民生活分析）與產業發展（金融、醫療AI）中的實際效益。這顯示合成資料已被視為在數據經濟時代下，平衡數據利用與個資保護的關鍵賦能技術。

（二）監理的挑戰與框架的建立：從法律到風險評估

會議中針對合成資料的法律地位與風險管理多有討論。E教授點出全球性的問題，即多數的既有法規並未明確定義合成資料，導致實務上傾向將其比照去識別化資料處理，卻缺乏一致的風險評估標準。J教授則分享韓國的因應方式，例如PIPC的指引體現了一種重要的監理趨勢：**不從技術本身定義其法律地位，而是要求透過一套嚴謹、可量化的風險評估程序來決定其資料屬性**。與會的專家多同意未來的方向應朝建立一套標準化、可操作的風險評估方法論前進，這是合成資料能否被信任並廣泛應用的前提。

（三）理論與實踐的權衡：效率與安全的抉擇

H副總裁從產業實務出發，提出「合成資料求快，真實資料求穩」的觀點。在自動駕駛這種不容許失敗的應用場景中，儘管合成資料

能以低成本、高效率的方式生成海量測試數據，但它終究是基於既有數據模式的模擬，可能無法涵蓋真實世界中未曾見過的黑天鵝事件。因此，在評估合成資料的效用時，必須依據應用的風險級別進行權衡。對於一般商業分析，合成資料或許已足夠；但對於涉及生命安全的關鍵系統，真實資料的驗證角色目前仍無可取代。

爐邊對談：人工智慧對醫療服務與隱私的影響（Fireside Chat:Impact of AI on Healthcare Services and Privacy）

爐邊談話主持人及與談嘉賓，由左至右分別為Ho Bae、Ran Balicer與Sooyong Shin。

主持人：Ho Bae（韓國梨花女子大學教授，Professor, Ewha Womans University）

與談人：

- Ran Balicer（以色列本·古里安大學公共衛生教授，Public Health Professor, Ben Gurion University）
- Sooyong Shin（Kakao Healthcare 首席研究官，Chief Research Officer, Kakao Healthcare）

本爐邊談話由韓國梨花女子大學Bae教授主持，他以現今人工智慧(AI)在醫療保健服務中的應用範圍廣泛，例如協助診斷、藥物研發、個人化健康管理及醫院智慧管理，然而，AI對於醫療領域既是機會亦是挑戰，目前已有技術例如假名化數據、解決方案、聯邦學習等方式以解決隱私風險。是以，本與談將聚焦於AI應用、合成資料、動態同意機制及政府隱私保護角色等四大面向，依序提問進行與談交流。

（一）AI對於醫療領域之變化及未來發展

首先由以色列本·古里安大學公共衛生B教授回應，AI並非醫療領域的新事物，例如以色列最大的醫療服務機構 Clalit Healthcare Services近15年來已導入智慧醫療AI模型。AI對醫療領域之最大效益，照護不再被動回應症狀治療，而是轉為積極預防，例如Clalit透過AI預測模型，協助識別丙型肝炎的效率提高約100倍。他認為這些進步未必需要仰賴應用最新之模型，反而傳統機器學習和深度學習技術即可實現。

接著，S首席研究官補充截至2025年7月，美國食品藥品監督管理局(FDA)已批准了101,247個AI醫療設備(AI medical devices)，但數據顯示這些設備中，只有2款設備獲得超過10,000次之保險理賠次數，這反映出醫療領域仍是相當保守。他提及生成式AI可透過聊天介面直接與病患對話，過往AI用以分析影像、檢驗數據，缺乏與病患之互動，現今得透過生成式AI蒐集病史、家族史等資訊可與電腦斷層掃描(computed tomography scan，CT)或磁振造影(Magnetic Resonance Imaging，MRI)等數據相互結合，以協助醫師和病患提供更有前景的診斷。儘管目前仍處於早期階段，但醫師與AI之協作將在不久的未來實現。

（二）醫療機構之AI應用及隱私治理

B教授預測，AI在醫療領域的應用將在一至兩年內顯著加速。他提及此趨勢的核心驅動力在於「不作為風險」已遠高於導入新技術的潛在風險。例如研究顯示，即便在先進的醫療體系中，仍有四分之一的住院病患因可預防的人為疏失而受害，爰管理者應重新權衡不導入AI所產生之持續性風險；而就數據治理層面，B教授亦引述以色列與德國的調查，高達八成的民眾願意讓自身健康數據在醫療保健領域被更廣泛地應用，反而與當前相對保守之法規限制或政治考量有所差異。

S首席研究官則從實踐層面補充，AI解決方案的可行性與成效取決於各國及個別醫療機構的具體條件，他提及韓國等已開發國家，其瓶頸可能在於醫院機構缺乏購置高階GPU的運算資源；而在低收入和中等收入國家，可能面臨缺乏穩定電力供應、伺服器或網路資料中心(IDC)，或許部署小型語言模型(SLMs)較更具成本效益與可行性。

（三）醫療數據之特殊性及保護措施

針對醫療數據是否應適用更嚴格的特殊保護規範，S首席研究官首先提出其觀點，他認為醫療數據具備高度敏感性且有必要監管之，但同時強調，相較於其他領域，醫療保健領域已存在一個成熟且嚴密的法規體系。他認為，現有法律框架的深度與廣度已足夠提供充分保障，無須再疊加額外的特殊規範。

B教授亦表示贊同，並補充醫療保健領域當前面臨的挑戰並非監管不足，而是「隱私過度監管」所帶來的負面效應。他擔憂這種現象

實質性地阻礙了技術創新與服務優化。在許多國家，部分機構甚至將隱私法規曲解為「不作為」的藉口，以此作為延遲必要之數位轉型與系統現代化的藉口。

（四）假名化、合成數據和聯邦學習等技術之優劣勢

S首席研究官指出假名化（pseudonymization)是使用醫療數據基礎且不可避免的方法。儘管各國都有類似的規定，但挑戰在於缺乏全球統一標準。即使在韓國，每家醫院應用不同的內部規定執行，反而提高跨國研究困難性，應制定全球指南或國際標準例如ISO 27000等；再者，即使數據經過假名化，在跨境傳輸時仍被視為個人資訊，跨國問題仍然存在；最後，他個人對合成數據(synthetic data)態度較為保守，因有時候該類數據之生成實務上不可能存在，反而僅能用以教育或模擬訓練。

然而，B教授則是樂觀其成，他認為縱有理論上的擔憂，但基於合成數據可創建較好的預測模型。合成數據有時也需要用於擴增小型數據集，以確保機器學習演算法能夠有效運作。他認為合成數據可用於加速開發，但於投入臨床實務前，須使用真實世界數據進行測試和最終驗證。B教授亦補充可應用差分隱私(differential privacy）技術等減輕再識別風險，以符歐盟通用資料保護規則(GDPR)等法規要求。

（五）動態同意管理(Dynamic Consent)之可行性

S首席研究官認為動態同意系統是非常必要且技術已成熟。他曾在醫院進行研究時實施該系統，證明它能有效管理患者的同意。例如，韓國國家生物樣本庫項目就採用了動態同意系統，以方便患者

輕鬆修改或撤回其同意的各個項目。他提出目前動態同意管理之困境，係患者一旦完成治療並離開醫院，就很難再取得他們對新的研究目的的同意。動態同意系統可以解決這個問題。

（六）可解釋性AI（Explainable AI, XAI）之透明治理

B教授認為取決於當下情境，舉例而言，黑箱模式(black box)適用於類似於自動化、技術性或手動流程的任務，只要結果經過測試且持續可重複，可作為黑箱機制運作，如同我們信任血液計數機器的結果；然而，可解釋性(explainability)適用於臨床上關鍵的決策過程或有意義的臨床困境，醫師排斥完全的黑箱，且需要能夠向患者解釋決策背後的生物醫學機制。他進一步以Clalit診所部署的AI系統舉例，該系統為基層保健醫師提供建議，且始終具備可解釋性，系統會解釋建議原因(例如血液檢測數值上升等)，醫師認為該系統提供安全感，讓他們感覺像是有心臟科醫師或內分泌科醫師在同一個房間內協助日常工作。

S首席研究官則同意醫療保健中的AI應該是可解釋的。但他強調，必須區分可解釋性(explainability)與可詮釋性(interpretability)，前者是理解為何做出這個決策，後者則是理解AI系統之內部運作方式，他認為不應對XAI施加過度負擔，即要求醫師像工程師一般理解模型內容。

（七）醫療領域及AI應用之交互影響

B教授認為醫療保健領域中運用AI，其優點在於AI將取代工作中具重複性、技術性、文書處理等瑣碎作業，讓他們能有更多時間進行富有同情心之人類互動；其次，良好治理機制將促進創新。由於A

I具有高度仰賴數據，類似藥品審查採集中式管理之政府層級未必適合。因此，治理責任應更多地轉移到組織層級，即醫院和衛生系統。最後針對病患而言，AI將使醫療保健普及化、民主化，讓大眾獲得安全、有效且主動預防性的最高水準護理。但最大的隱憂則是AI系統的關鍵性提高，以至於會成為惡意組織或國家級別攻擊的目標區域。這種風險將會增加，並可能限制我們最大化利用創新的能力。S首席研究官則認為樂觀和悲觀的觀點是同一件事，即AI醫生提供的醫療護理。最終結果取決於「AI醫生」如何被負責任或合理地被使用。

總結而言，本次對談確立了一個清晰的治理方向：驅動醫療AI發展的關鍵，已從被動的法規遵循，轉向主動的「信任建構」，這意味著責任的主體正從政府的單一監管，延伸到醫療機構的自主治理與在地化驗證。因此，我們必須在技術上推動數據流通的全球標準化與患者的動態同意賦權；實務上則須務實評估合成數據等新興工具的價值與極限，並根據風險高低，匹配相應的AI可解釋性。最終目標是構築一個以病患為中心、兼具倫理韌性與創新活力的數據生態系，讓預防性照護的潛力得以安全、負責地實現。

主題演講二（Keynote 2）

歐盟民主、司法、法治與消費者保護專員Michael McGrath演講

本場次由歐盟民主、司法、法治與消費者保護專員 Michael McGrath（Commissioner for Democracy, Justice, the Rule of Law, and Consumer Protection，任期為2024－2029）發言，本次亦為他首次出席全球隱私大會（GPA）。M委員在致詞中指出，GPA是討論與制定資料保護政策的重要平台，尤其在人工智慧（AI）革命開啟「未知水域」之際，資料保護機構（DPA）的角色至關重要，確保公民權利不僅止於書面規範，而能在實踐中獲得保障。

（一）歐盟AI法制進程

M委員強調，現下歐盟正透過以人為本的法規來引導AI創新。歐盟的《人工智慧法案》（AI Act）已於2024年8月1日正式生效，該

法案的規範將於未來三年內分階段適用，其中針對通用AI 模型的風險管理規則，已自2025年8月開始實施。歐盟委員會並已發布《通用AI行為準則》（Code of Practice on General-Purpose AI），以確保前沿通用AI模型的透明度與安全性，目前已有27家供應商(providers)簽署，其中包含OpenAI和Google。

（二）歐盟AI相關政策

今（2025）年四月，歐盟提出AI行動計畫（AI Action Plan），針對新創、擴大企業及中小企業擴大公共AI基礎設施，並將以AI工廠(AI factories)的方式提供給這些企業，預計於2026年底前至少有15座AI工廠投入營運。此外，歐盟亦已啟動 AI Pact 網路（涵蓋超過 3,000 名參與者）及 *AI Act 服務台（AI Act Helpdesk）。在國際合作層面，歐盟將持續引領AI治理規範的發展，並與韓國、日本、新加坡、印度、加拿大及美國等夥伴保持緊密合作。

（三）歐盟消費者權益與監管措施

M委員重申，AI創新必須保障消費者的權利，因此歐盟提出相關配套規範，如《消費者信貸指令二》（Consumer Credit Directive II, CCD II）要求自動化資料處理下的個性化服務須具備透明度，並引入人工監督機制。歐盟委員會本身也善用AI工具（如EU eLab）以加強消費者保護與執法。歐盟正考慮於《數位公平法案》（Digital Fairness Act）中增訂條款，要求企業確保所有客戶在與AI系統互動時，均可選擇與真人代表對話，以避免任何族群被科技浪潮給遺漏。

（四）展望未來

最終，M委員以一句話點明核心：「沒有資料保護，就沒有值得信賴的AI。」他指出，歐盟的《一般個人資料保護規則（General Data Protection Regulation, GDPR）》是所有涉及個人資料處理的歐盟數位法律基礎，與《AI 法案》互為強化。他強調創新與隱私並非對立，而是相互促進、相互強化的關係。他對GPA的未來抱持信心，認為透過全球協作與共同思考，AI將能為全世界公民帶來實質益處。

場次四（Panel Session 4 ）：為人工智慧目的處理個人資料的合法性（Lawful Bases for Processing Personal Data for Purposes of AI）

主持人與與談嘉賓，由左至右分別為Bojana Bellamy、Anu Talus、Beatriz de Anchorena、Dale Sunderland、ByoungPil Kim

主持人：Bojana Bellamy[7]（資訊政策領導中心主席，President, Centre for Information Policy Leadership）

與談人：

- Anu Talus（歐洲資料保護委員會主席，Chair, EDPB）
- Beatriz de Anchorena（阿根廷個人資料保護局局長，Titular(Head), AAIP, Argentina）

[7] 主持人經歷請參CIPL官網：https://www.informationpolicycentre.com/bojana-bellamy.html

- Dale Sunderland（愛爾蘭資料保護委員會委員，Commissioner, DPC, Ireland）
- ByoungPil Kim（韓國科學技術院教授，Professor, KAIST）

本場次聚焦於AI時代下，傳統資料保護法規面臨的挑戰與調適，相關議題討論如下：

（一）適法性基礎的再思考：以「正當利益」為核心

與談者普遍認為，在AI訓練這種涉及海量資料、目的動態演變的情境下，傳統以「同意」為主的適法性基礎已顯不足。相對地，「正當利益(legitimate interest)」被視為更具彈性與可問責性的選項。從愛爾蘭DPC推動EDPB提出意見，到韓國PIPC發布指引，監管機構正積極為如何落實「正當利益評估」提供框架，要求開發者在主張自身利益的同時，必須證明其已採取足夠的技術與組織措施來保障個人權利，達成實質的平衡。

（二）「目的拘束原則」的演進：從嚴格限制到風險導向

AI的出現直接挑戰了「目的拘束原則」。與談者並未主張廢除此原則，而是探討如何使其更具彈性。愛爾蘭資料保護委員會S專員主張將其納入整體的風險評估框架中，根據個案情境、個人合理期待與風險緩解措施進行綜合判斷。韓國科學技術院K教授則提出更具體的兩階段論，認為隱私風險包括靜態的「訓練資料」以及動態的「執行階段資料」，因此監管的重心也應隨之轉移，對前者放寬，而更著重如何應對後者。

（三）「特種個資」的雙重困境：保護與偏誤緩解的兩難

特種個資是AI發展中最棘手的議題。一方面，法律對其處理有著最嚴格的限制，如韓國的案例所示，未經同意的使用將直接面臨裁罰；另一方面，為了偵測與消弭AI的偏誤與歧視，又恰恰需要這類資料。歐洲資料保護委員會T主席指出，歐盟《人工智慧法（AI Act）》已開始針對此一兩難局面尋求解方，為具備重大公共利益的目的尋求合適的法律解釋，顯示監管正試圖在嚴格保護與合理使用之間尋找新的平衡點。

（四）監管的未來：從法規遵循到協作治理與技術賦能

整場討論的共識是，面對AI的快速演進，單靠傳統的監管已不足夠。與會者一致強調**公私協力**與**跨國合作**的重要性。同時，除了法律層面的探討，與會者也對技術的潛力抱持希望。K教授提出的「多代理人AI系統」概念，暗示了未來的AI或許可透過「自我辯論」與「過程紀錄」，內建更高程度的透明度與可解釋性，從而使法律遵循更具實效性。這也呼應了阿根廷個人資料保護局A局長所提倡的，監管者應扮演「責任創新的驅動者」，引導技術朝向更符合人類價值的方向發展。

平行論壇1-A（Parallel Session 1-A）：新興設立與制度化資料保護機構（由APPA主導）Newly Establishing and Institutionalizing DPAs (led by the APPA)

1-A與談現場嘉賓，由左至右分別為Denise Wong、Janghyuk Choi、Michael Webster、Pansy Tlakula、Taylor Reynolds。

主持人：Denise Wong（新加坡個人資料保護委員會副主席，Deputy Commissioner, PDPC, Singapore）

與談人：

- Janghyuk Choi（韓國個人資料保護委員會副主席，Vice Chairperson, PIPC, Korea）
- Michael Webster（紐西蘭隱私專員辦公室隱私專員，Privacy Commissioner, OPC, New Zealand）

- Pansy Tlakula（南非資料保護委員會委員，Chairperson, IRSA, South Africa）
- Taylor Reynolds（世界銀行代表，Practice Manager, World Bank）。

本場次由新加坡W副主委主持，旨在探討資料保護機構（Data Protection Authorities, DPAs）的設立過程、營運挑戰與制度化進程。主持人於開場指出，**根據最新統計，自2021年至2024年間，全球資料保護法規成長幅度達10%，現已涵蓋超過160個國家，其中近八成已投入資金、能力建構與人才培訓**，並逐步形成制度化架構。她同時強調，區域合作平台如亞太隱私機構（APPA）與東南亞國協（ASEAN）已成為經驗交流與政策協調的重要場域，對於強化新興DPA的能力發揮了積極作用。

（一）DPA的設立與制度化挑戰

世界銀行R代表指出，根據廣泛調查，歸納DPAs在設立與營運過程中普遍遭遇的五大挑戰。**首先是資金不足與獨立性欠缺**，逾七成的機構坦言經費來源不足，難以維持持續性運作，且在制度設計上往往受制於政府部門，影響其獨立監管職能。其次是*專業人員匱乏與培訓不足*，許多國家缺乏相關教育資源，導致監管人力短缺。第三，**執法資源極度有限**，使得機構必須選擇性處理案件，而非全面性執行法規。第四，**社會與政府部門對DPA的重要性認知不足**，如何提高公眾及決策者之意識，成為重大挑戰。最後，DPAs的職權範圍不斷擴張，除資料保護外，近年更被要求**承擔人工智慧（AI）監管的責任**，並需參與跨部會數據治理計畫。

南非T主席進一步以其國家實例加以說明：並說明IRSA成立於2016年，草創階段既無資金亦無人員，委員彼此間甚至缺乏先前合作

經驗。該機構最初必須借鑑英國、加拿大與德國的先行經驗，並自行起草法規與指導方針。由於早期依附於司法部的政策與ICT系統運作，其獨立性曾受質疑。然而，當司法部遭遇勒索軟體攻擊後，IRSA毅然展開調查並最終裁罰約25.8萬美元，此舉不僅彰顯其職權，亦確立了作為獨立機構的地位。然而，其法律制度存在語意晦澀與適用遲滯的問題，執法權直至五年後的2021年方才生效，而首宗訴訟（針對教育部未經同意發布學生成績）亦於同年10月正式展開。

紐西蘭W專員Michael Webster強調，DPAs的框架應根據不同國家的政治、經濟、社會與文化結構加以設計。他指出，**獨立性、資源配置、職權範圍、資金來源以及監管立場，為影響DPA能否有效運作的五大核心要素。**

韓國C副主席則介紹該國的轉型經驗：自2020年起，PIPC正式成為獨立的綜合性DPA，並引入一系列新制度，包括隱私政策驗證、資料可攜性規範，以及跨境資料傳輸暫停權，該制度類似於歐盟適足性決定。此外，韓國亦賦予個人挑戰AI自動化決策之權利，以確保AI應用符合資料保護原則。

（二）監管策略與應對模式

在探討監管策略時，紐西蘭W專員提出「**懸崖頂上的防護欄，而非懸崖底下的救護車**」之哲學，主張**透過教育與參與來預防問題發生，而非僅於事後處理個案**。他建議監管機構應使用商業語言向社會與決策者說明隱私保護的價值，例如大規模資料外洩所造成的數千萬美元成本，或高層官員因資料洩露而蒙受政治壓力。此外，紐

西蘭更要求各組織設立「隱私官」，以確保隱私保護在內部治理中落實。

南非T主席則說明其因應資源不足的多元策略，包括推動修法以保留部分罰款收入、與公司註冊機構合作建立資訊官員註冊制度並收取費用、以及推展「監管機構走向基層」計畫，深入偏遠社區以簡單語言普及隱私保護概念。

韓國C副主席也說明韓國於2023年發表AI政策方向文件，建立AI風險隱私管理模型，目的在於同時促進技術創新與保障個人權益。

世界銀行R代表也提出世界銀行的分階段發展模式，建議新興DPA在第一階段（1至3年）專注於制度架構建構與社會意識提升，於第二階段（4至8年）則逐步加強執法與跨部會合作。他特別指出，DPAs必須確保制度上之獨立性，以避免受制於政府更迭而失去持續性。

（三）國際合作的重要性

與會各方一致認為，**國際合作是DPA制度化發展的重要支柱**。紐西蘭W專員以澳洲與紐西蘭因應大規模資料外洩事件之聯合調查為例，強調跨國合作能夠有效提升執法成效。韓國C副主席則提到，韓國在處理跨國平台公司（如ChatGPT）之違規時，會與歐洲監管機構諮詢合作，並進一步將IMEI結合使用者數據視為個人資訊。南非T主席則疾呼全球隱私保護組織GPA應採取集體行動，以共同制衡違反多國法律之跨國企業。世界銀行R代表則表明，世界銀行在隱私治理上將維持中立，並依據各國具體需求提供不同模式的最佳實踐案例。

最後，主持人新加坡W副主委總結指出，各國雖處於不同的發展階段，但DPAs所面臨的挑戰卻具有高度相似性。透過國際論壇、雙邊對話以及世界銀行等多邊機制的協助，DPAs能夠相互學習，並逐步建立健全而具韌性的制度。她強調，未來的發展方向**應著重於制度化保障、跨國合作以及科技治理**，方能因應快速變動的數據環境與科技挑戰。

平行論壇1-B（Parallel Session 1-B）：人道行動中的資料保護十年回顧（由WG AID主導）（10years of Data Protection in Humanitarian Action: Building on the past to navigate future challenges for Humanitarian Action in the age of AI (led by the WG AID and the ICRC)）

1-B論壇與談現場

主持人：

Massimo Marelli（國際紅十字會資料保護辦公室主任，Head, Data Protection Office at ICRC）

Catherine Lennman（瑞士聯邦資料保護與資訊專員國際事務與法語事務代表，Delegate for International Affairs and Francophonie, FDPIC）

與談人：

- Beatriz Anchorena（阿根廷個人資料保護局委員，Commissioner, AAIP, Argentina）
- Carmen Casado（聯合國世界糧食計劃署全球隱私辦公室主任兼資料保護長，DPO and Director of the Global Privacy Office, UN World Food Programme）
- Youngsu Jong（韓國個人資料保護委員會資深副處長，Senior Deputy Director, PIPC, Korea）
- Immaculate Kassait（肯亞資料保護委員辦公室，Data Commissioner, ODPC, Kenya）
- Hiroshi Miyashita（日本中央大學政策研究學部副教授，Associate Professor, Faculty of Policy Studies at Chuo University）
- Cosimo Monda（荷蘭馬斯垂克大學歐洲隱私與網路安全中心主任，Director of the Maastricht European Centre on Privacy and Cybersecurity, Maastricht University）
- James De France（紅十字會與紅新月會國際聯合會法務主管兼隱私保護辦公室負責人， Managing Legal Counsel and Head of the Data Protection Office, IFRC）
- Alex Novikau （聯合國難民署資料保護與隱私事務主任，Chief Data Protection and Privacy Officer, UNHCR）
- Wojciech Wiewiórowski(歐洲資料保護監督機關專員，European Data Protection Supervisor, EDPS）

本次平行論壇1-B主持人及現場與談嘉賓，從左至右分別為：Massimo Marelli、Carmen Casado、Alex Novikau、James De France、Immaculate Kassait、Beatriz Anchorena、Wojciech Wiewiórowski、Hiroshi Miyashita、Soyoung Yoo、Cosimo Monda、Sooyong Shin、Catherine Lennman。

本與談由國際紅十字會資料保護辦公室M主任及瑞士聯邦資料保護與資訊專員國際事務與法語事務L代表共同主持，主持人L代表指出今(2025)年是國際人道行動個資保護之重要里程碑，2015年國際紅十字會(ICRC)通過首份個資保護規章，聯合國難民署(UNHCR)亦制定其個資保護監管框架，同時全球隱私大會(GPA)則通過關於「隱私與國際人道行動」的決議，十年後這三個組織即將於12月出版《資料保護於人道行動：在數據驅動的世界中回應危機》一書，集結各方人道組織、個資保護機構及學界專家之觀點，凸顯在人道救援行動中(例如戰亂、危機時刻中)個資保護之重要性；此外，國際紅十字會亦針對其出版之《人道行動中的資料保護手冊[8]》進行多語言翻譯，包括西文、法文、中文、日文及韓文等，以供各國人道行動下個資保

[8]手冊內容詳 https://www.icrc.org/zh/document/data-protection-humanitarian-action

護之參考。主持人M專員補充人道行動下許多脆弱地區，個資保護制度可能根本不存在，即便建立制度，執行亦有其困難，爰需要藉由組織合作將個資保護帶入這些最需要卻又易被忽略的地方，本與談之核心議題綜整如下：

（一）隱私可以救命－論人道行動下資料保護之特殊性

聯合國難民署資料保護與隱私事務A主任強調人道行動中，**受助者的資料保護正面臨極端存在的風險及權力不對稱**，例如武裝衝突下的難民等，而此情境下資料處理活動相當多元，例如國際紅十字會處理基因資料協尋失散親人、聯合國難民署與各國政府協調建立庇護機制、難民登記等，均是涉及高度敏感個資處理活動，而因**涉及個資處理範圍及活動甚為龐雜，顯示人道行動下之個資保護特殊性及差異性**，亦須仰賴國際手冊等共同指引據以依循。

聯合國世界糧食計劃署全球隱私辦公室C主任兼資料保護長提及人道活動其實受到數位轉型影響深遠，她強調「**隱私可以救命**」，當面臨武裝衝突或戰爭情境下，倘被登錄為受助者而被辨識出身分者，就可能成為攻擊目標，而女性風險更高，甚至人道工作者本身也可能成為攻擊對象；隱私保護並非目的，而是確保人道行動能夠進行的手段，而透過數位轉型協助人道行動之推展，惟更多科技導入，隱私所產生之風險亦隨之增加，故在利用科技當下，實務工作者亦須反思如何持續降低隱私風險，其關鍵在於打造負責任的科技(Responsible Technology)、建立負責任的合作機制(Responsible Cooperation)及培訓與意識建立(Training and Awareness)。她強調隱私導入技術是前提而非附加事項，須跨組織合作而非單打獨鬥。

歐洲W資料保護監察專員則提及透過人道組織之合作讓他學會謙卑，從起初以為人道行動就是眾多部門之一而已，**後來發現在人道領域中，任何一個疏失可能都會關乎生死**，例如組織在戰區處理資料、提供救援時，若因疏失洩露資訊，可能導致當地武裝勢力利用資料去追殺平民，因此對資料保護主管機關而言，人道行動絕非一般議題，即使所在國家沒有戰爭或災難，可能也會需要處理相關案件，他比喻現實中律師犯錯還可上訴，但醫師疏失可能關乎生命安全，資料保護官在人道行動領域裡亦是扮演關鍵角色。

（二）人道行動之資料跨境傳輸及在地實踐

紅十字會與紅新月會國際聯合會法務主管兼隱私保護辦公室J負責人提及人道行動下的跨國資料傳輸亦是關鍵，現場實務者面臨的複雜性更多，目前得以藉由多種通訊平台串接、同時運作，但亦增加法律與技術之困難度，例如過往以紙本問卷蒐集資料，現在透過電子表單或自我登錄(self-registration)應用程式處理，但隨之問題產生，某些地區受限於沒有智慧型手機或網路，可能導致受助者無法獲得協助，因此**資料傳輸與技術難題，不僅關係於隱私與尊嚴，更影響著實務工作者如何快速且有效提供服務予受助者**。

阿根廷個人資料保護局委員兼伊比利美洲資料保護網絡(RIPD)B主席分享區域合作之觀點，《歐洲資料保護公約 108+》第5條提及資料處理須兼顧比例原則及依法行政，例如疫情、天災或武裝衝突等緊急狀況下得基於特殊目的處理個資，但**原則確保即使在危機中，亦須兼顧人的尊嚴與基本權利**。就拉丁美洲而言，我們強調要讓這些國際標準結合在地脈絡，例如阿根廷雖非戰區，但貧困率高達40%，仍存在教育與數位落差，因此資料保護須強調地方透明治理，例

如持續與申訴專員辦公室合作，針對兒童及公務員推動隱私權教育並建立公部門DPO網絡，以建立負責任的資料文化；另伊比利美洲資料保護網絡（RIPD）則針對數位暴力、生成式AI等主題建立工作小組，並與大型科技公司協調建立緊急通報管道以保障弱勢族群。**國際標準必須與地區與在地行動結合，才能真正讓人道理念落地**。

（三）人道行動未必有硝煙-災害情境下之隱私治理

日本中央大學政策研究學部H副教授補充，除了上開人道行動聚焦在戰爭或武裝衝突之緊急情境，亦包括天然災害及人為災難。根據2023年全球災害報告，亞洲地區的災害事件數量占全球42%以上，因此推動人道規範與資料保護也更為珍貴。回顧GPA曾有2個重要里程碑，一是2015年阿姆斯特丹會議通過的《隱私與國際人道行動決議[9]》;另一是2011年由紐西蘭主導的《自然災害中的資料保護決議》，當年日本與紐西蘭分別歷經東北311大地震及基督城地震，後續東協(ASEAN)也依循這些精神，制定了災害管理與應變協定，可見人道行動及隱私保護已不再分離。例如日本經歷地震後，各避難中心以手寫名單紀錄失蹤者，並透過上傳網路協助親屬協尋，惟此公告姓名、年齡、地址等個人資料亦產生隱私疑慮。

韓國個人資料保護委員會Y資深副處長提及，韓國稱人道行動為緊急應變(emergency response)，係強調公民責任的義務而非慈善心態，例如2015年韓國爆發MERS-CoV疫情，當時缺乏法律依據蒐集必要個人資料，故即時修法因應疫情；惟近年面臨嚴峻COVID-19疫

[9] 此決議係於2011年全球隱私大會第33屆國際會議發布。內容詳：https://globalprivacyassembly.com/wp-content/uploads/2015/02/Resolution-on-Data-Protection-and-Major-Natural-Disasters.pdf

情卻面臨不同問題，即使已有法律基礎，反而因過度蒐集或揭露個資遭人詬病。上開經驗顯示即使面臨緊急狀況亦須遵守資料保護原則，避免不必要之侵害，因此韓國後續推出災害應變、傳染病防治、失蹤人口協尋及金融詐騙等四大情境指引，期以在推展人道行動之同時，也能尊重基本權益及人類尊嚴。

（四）從第一線開始努力-論人道行動實務工作者之個資保護意識深化

肯亞I資料專員延續說明人道領域中資料保護之複雜性，人道行動會受到各國之法律拘束，因此人道工作之兩難在於一邊保護受害者資料，一邊面對政府以國家安全之名義要求提供資料。因此監管機構必須主動提供指引，鼓勵組織自律及自我監管，採用區域性共同條款(regional clauses)促進跨國合作及協調，並持續深化能力培育與意識提升，例如讓現場人員理解現場不應蒐集過多資料、資料再利用產生更多風險等。畢竟人道行動現場無法完整執行資料影響評估（DPIA），但其關鍵角色在於預先識別與嘗試減輕風險。

荷蘭馬斯垂克大學歐洲隱私與網路安全中心C主任以人道行動者培訓之獨特性作為結語，很多人起初可能會說忙著救人哪來時間處理資料保護，但**必須讓他們認知人道領域之獨特性、面對真實情境的兩難及實用導向，才能建立信任關係提供有效援助**；另外與國際組織協力合作，畢竟數位時代任何行動會留下足跡，同時亦須關注如何讓數位素養(digital literacy)持續深化。

綜上，人道行動與個資保護並非二事，須兼顧極端情境之特殊性及基本隱私權之保障，唯有在地落實(前線人員培訓)、跨域合作(數位轉型)及國際監管機制及持續對話，才能在人道行動之實務認知個資保護之重要性。

平行論壇1-C（Parallel Session 1-C ）：在人工智慧時代重新思考資料保護法（由隱私權未來論壇FPF主導）（Rethinking Data Protection Law in the Age of AI (led by the FPF)）

主持人及現場與談嘉賓，由左至右分別為Gabriela Zanfir-Fortuna、Carly Kind、Christopher Kuner、Sangchul Park、Monika Tomczak-Górlikowska。

主持人：Gabriela Zanfir-Fortuna（隱私未來論壇副總裁，Vice President, Future of Privacy Forum）

與談人：

- Carly Kind（澳洲資訊專員辦公室專員，Commissioner, OAIC, Australia）
- Christopher Kuner（丹麥哥本哈根大學教授，Professor, University of Copenhagen）

- Sangchul Park（韓國首爾大學教授，Professor, Seoul National University）
- Monika Tomczak-Górlikowska（Prosus 公司首席隱私長，Chief Privacy Officer, Prosus）

本場平行論壇係以「AI時代下資料保護法制的反思」為核心，聚焦在人工智慧（AI）快速發展的時代，過去半世紀以來形成的資料保護法律原則（如目的限制、資料最小化及資料主體權利）是否仍然適用，或是否應進行調整乃至制度性改革，與會專家從學術、監管與實務等多元視角進行討論，重點摘錄如下。

（一）資料保護法的原則性與彈性：從歷史脈絡看AI時代的法制延續

哥本哈根大學K教授從歷史脈絡切入指出，資料保護法的誕生可追溯至1960年代末期，起因於當時電腦化資料收集與資訊處理的技術進步。惟隨著資料的電腦化與集中化，社會開始意識到個人資訊被濫用的風險，而資料保護法正是為了在技術創新與人權保障之間建立平衡而誕生。

其認為資料保護法之所以能在數十年來持續發揮作用，關鍵在於此套法制被設計為「基於原則」（principle-based）的監管體系，其高層次的指導原則，例如目的限制（Purpose Limitation）與資料最小化（Data Minimisation），在設計上就具備高度的彈性（flexibility）和適應性（adaptiveness），旨在具備足夠的彈性以因應科技環境的變遷。因此在AI時代下，尚無需對資料保護的基本原則進行根本性（fundamental）的改變。

隨後，K教授強調，AI的出現帶來廣泛討論與監管焦慮，目前公共與立法討論存在一種「監管炒作」（regulatory hype）或「監管泡沫」（regulatory bubble）的現象，社會對AI的關注與恐懼被放大，導致大量法規與政策被倉促提出。然而，他認為AI並未帶來根本上全新的法律問題，AI應用確實具有其獨特性，但其中多數挑戰是現有資料保護原則框架下可調適的範疇。

其進一步指出，AI的許多應用實際上並不涉及個人資料，例如軍事用途中利用AI協調無人機群的案例，與資料保護法關聯則非常有限。AI的發展正在挑戰我們對「什麼是資料保護」這個概念的邊界，許多與AI有關的監管問題其實超出資料保護範疇，涉及倫理、競爭法與消費者保護等面向。因此，監管機構未來將不得不考慮跨領域合作或擴大職權，以應對AI所引發的更廣泛治理議題。整體而言，Kuner教授呼籲與其進行高風險、充滿政治爭議的修法，不如透過更靈活、合理的法律解釋與實務應用，在保護個人權利與促進創新之間尋求平衡。

（二）全球企業治理挑戰：AI 時代下的速度、技術與依賴風險

再來，Prosus公司T隱私長以其長年在跨國企業法遵與隱私治理領域的實務經驗角度出發，強調當前面對AI的挑戰並不在於重新思考資料保護法本身，而是資料保護專業（data protection profession）和資料保護治理（data protection governance），並明確指出了當前實務中面臨的三大核心挑戰：

1、 速度挑戰（The Speed Challenge）

首先是AI發展的速度已遠超傳統隱私治理與風險評估流程的步調，資料保護管理者必須具備「敏捷性」（agility）與「決策的勇氣」（courage to decide），否則將被時代淘汰。在AI產品的快速迭代中，隱私與法遵團隊往往被迫在有限時間內做出判斷，專業人員必須具備更高的風險辨識能力與決策果斷力。若法遵團隊仍以傳統「等待明確規範」的方式處理問題，將無法跟上技術開發的節奏。

2、 **技術複雜性**（Technical Complexity）

AI系統的運作與決策過程極度複雜，單憑法律專業已難以充分掌握其潛在風險，未來的資料保護專業將是一個融合法律、技術與倫理判斷的跨域職能，資料保護人員必須具備跨領域的技術素養與開放學習的態度（openness to learn），只有深入理解AI模型的運作原理、訓練資料結構與風險來源，才能真正識別風險。

3、 **基礎設施集中化與依賴性**（Concentration and Dependency in Infrastructure）

全球絕大多數AI的基礎層技術高度集中於少數大型科技供應商，此種基礎設施的集中化，導致處於應用層的企業（特別是在全球南方國家，如印度、拉美等地）對於底層技術的隱私保護設定幾乎沒有影響力，形成了技術與合規上的嚴重依賴。Tomczak-Górlikowska呼籲全球社群應致力於打造更民主、更多元的技術生態系（more democratic and diverse technological ecosystem），以避免技術權力的集中，降低單一供應鏈帶來的治理風險。

除了上述三大實務挑戰外，T隱私長也強調了監管協調的重要性，**並特別提到歐盟《人工智慧法案》（EU AI Act）即將生效，這**

將使監管協調成為關鍵議題。由於AI的監管涉及多個機構，包括資料保護機關(DPA)、新成立的AI辦公室、網路安全機構以及其他部門監管機構，若缺乏「明智的協調」（wise coordination），企業可能面臨繁複的多重通知與溝通管道，耗費大量時間與資源，反而可能對創新造成負面影響。因此呼籲建立高效協調機制，將是確保法規順利實施並促進創新的關鍵。

（三）後AI專法時代的監理實踐：以指引落實原則、以行動塑造信任

澳洲K專員接續從監管實務角度分享澳洲的經驗與觀點，其指出許多國家現已錯過為AI制定獨立法律的時機，因此在缺乏 AI 專法的情況下，監管者的任務是明確闡釋現有法律如何適用於AI，為企業提供確定性」（certainty）與明確的行動指引。

其並提出澳洲的《隱私法》（Privacy Act）屬於高度「基於原則」（principle-based）的法制架構，因此OAIC的策略是透過具體指引，說明AI情境下如何落實此些原則。OAIC近年發布了兩套具體指引，分別針對**開發與訓練AI模型**（developing and training AI models）以及**使用現成商業AI工具**（using commercially available AI tools）的情境，一方面將模型訓練定義為「次要目的」（secondary purpose）並要求合法性評估；另一方面提醒輸入個資至市售AI工具時可能構成「第三方揭露」（disclosure），企業必須證明符合資料主體合理預期。

她舉例醫療影像企業案例：該公司將3000萬筆病患資料提供AI公司進行模型訓練，經匿名化後不再受《隱私法》拘束。OAIC透過公開調查報告，提供可操作的合規準則。

K專員同時提出「監管者即顛覆者」（Regulators as Disruptors）的理念，主張監管機構應主動透過執法與指導行動影響技術發展方向，以回應社會對 AI 的信任需求。然而，監管者自身亦面臨三大結構挑戰：**技術專業不足、調查權限落後與救濟機制不明確（如模型銷毀問題）**。她強調，AI 治理需跨越隱私、倫理與競爭法邊界，推動跨域協作與制度創新。

（四）法制轉型與監管重疊：韓國資料保護修法的制度新局

P教授以韓國為例，指出韓國政府正修訂《個人資訊保護法》（Personal Information Protection Act, PIPA），試圖為AI創新提供更明確的法律依據。此次修法的核心精神，是在特定保障措施下，更廣泛允許原始個資被用於AI開發，而不再要求事前去識別化或假名化處理。

回顧韓國個資保護制度的演進脈絡，在早期的監督式學習（supervised learning）階段，AI 所使用的資料多為結構化資料（structured data），通常儲存在資料庫中，使得「假名化（pseudonymization）」得以成為一項獨立且穩定的合法處理依據。韓國的個資主管機關—**個人資料保護委員會（PIPC）**，也曾以假名化資料為核心，建立出一套監管框架。然而在大型語言模型（LLM）與生成式 AI出現後，AI模型訓練多依賴非結構化資料（unstructured data）包括如文字、影像、音訊等，傳統的假名化技術已無法應用。

在此背景下，韓國開發者與產業界不斷向政府反映，現行制度缺乏足夠的法律確定性（legal certainty），尤其是在 AI 模型訓練階段如何合法使用原始個資的問題方面，PIPC為了回應產業界對

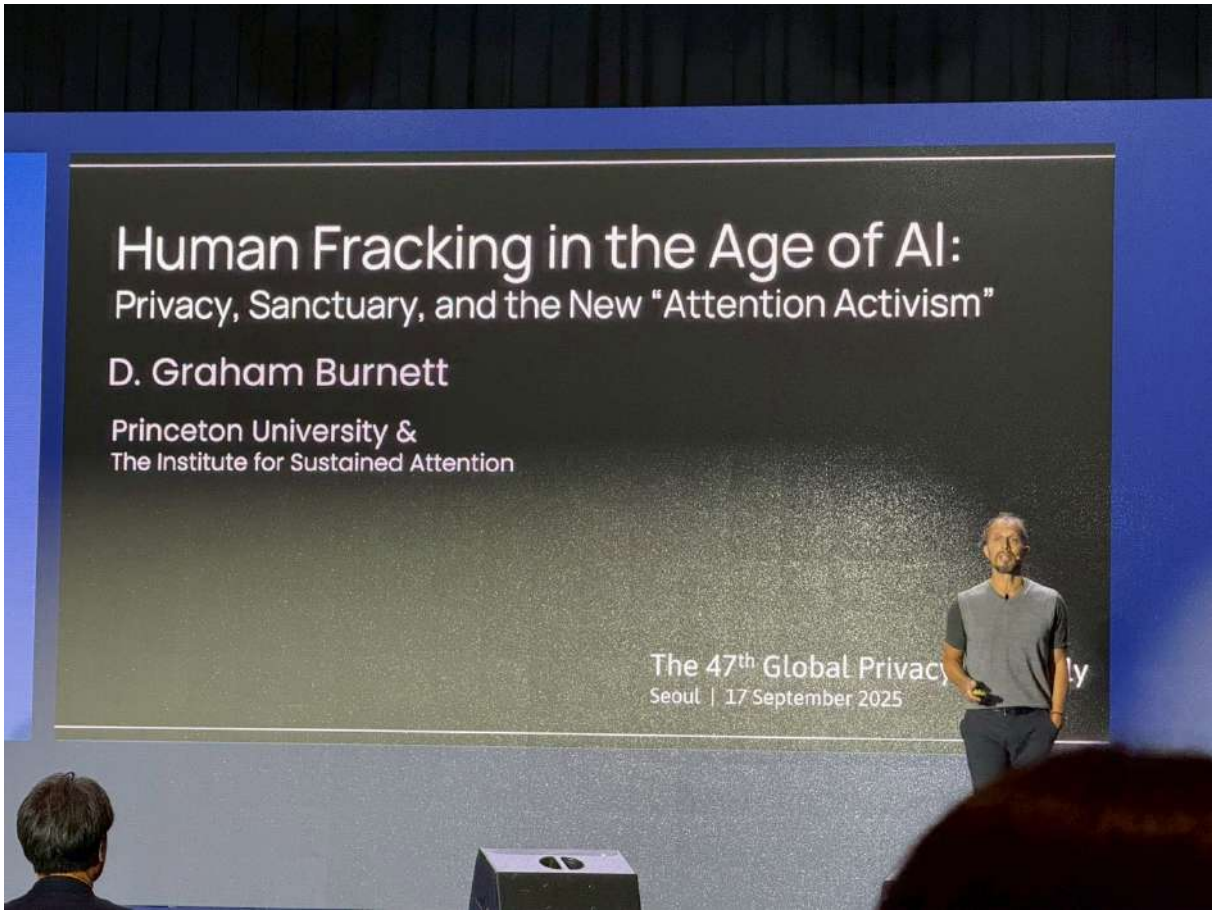
「法律確定性」的需求，也啟動了**正式的修法程序**，希望透過立法明文來解決制度瓶頸。

P教授指出，本次 PIPA 修法的**核心精神**，在於**允許更廣泛地將原始資料用於 AI 開發目的**，並將此種AI開發使用視為「**相容目的**（compatible purpose）」的一種合法資料再利用。換言之，只要資料處理者在開發 AI 時採取了特定的安全與保護措施，便可在不進行去識別化而合法地進行資料再利用。

然而，P教授也指出，此種作法雖有助於降低企業合規負擔、提升AI研發動能，但同時可能衝擊現有的利益衡量與權利平衡機制。因此其適用前提是「採取了一些特定的安全措施，並且存在某些合法利益」，具體做法可能包括要求進行事先審查（prior check）等等，以確保在創新與保護之間取得平衡。

P教授也提及儘管修法為產業提供法律確定性，但韓國在 2024 年通過了《人工智慧基本法》（AI Basic Act），成為亞洲少數同時擁有**AI專法與資料保護法**的國家之一，兩部法律的互動關係仍在形成中，但潛藏著的監管重疊與權限界線問題，AI基本法由科學技術資訊通信部主導，為避免與PIPA的監管重疊，該法排除「部署者」（deployers）的監管概念，使AI創作者或提供者成為主要受監管對象，雖此舉能減少與現有資料保護法的衝突，但如果提供者扮演資料處理者的角色，仍然可能存在監管重複。此外，韓國對自動化決策（automated decision-making）有嚴格的監管，也可能在兩部法律互動時引起一些問題。

主題演講三（Keynote 3）



普林斯頓大學教授D. Graham Burnett演講

本場次由普林斯頓大學教授 D. Graham Burnett進行演講，主題為「**人工智慧時代下的人類壓裂：隱私、庇護及新注意力行動主義**」(Human Fracking in the Age of AI: Privacy, Sanctuary, and the New "Attention Activism")，旨在釐清當代隱私保護的歷史脈絡與制度基礎，並從注意力經濟（attention economy）出發，探討其與人工智慧發展下的社會風險。

（一）注意力經濟的歷史奠基

B教授先以自身史學背景開場，其主要研究科技及科學史，過去幾年專注於**探討人類注意力如何從實驗室中被研究的歷史**。他指出，

今日廣泛討論的注意力經濟並非突然出現，而是深植於二十世紀中葉實驗室研究的傳統。

早在1930至1940年代，特別是早期類比機器（analog machines）驅動的眼球追蹤技術（eyetracking），運用於追蹤人們在影像上的注視路徑為何，當時實驗室研究資金主要源自廣告業及軍方，廣告業關注消費者在男性服裝廣告上注視的具體位置，以優化廣告設計及商業行銷，軍方則致力研究於人類在雷達監控下長時間維持警覺的能力，以精進軍事作戰效率等。當時，人類注意力從實驗室研究開始逐步被量化(quantification)及具體化(objectification)，進而被數據化(datafication)。換言之，現今隱私爭議緣自人類注意力長期被商業與軍事利益轉化為數據資源之過程。

（二）人工智慧時代下的「人類壓裂」

B教授表示他以兩種身份出席，一是對人類注意力如何轉化為數據有深入瞭解的教授，二是認為對人類注意力的理解是人類繁榮（human flourishing）注意力行動主義者。他認為，在社會規模的數位平台上保護人類數據，與人類繁榮之間存在密切關係。

他提出本次演講的主要核心概念即「人類壓裂」（Human Fracking），這是借鑑於石油壓裂技術（petroleum fracking)的比喻，現今資本雄厚且善用心理學的科技巨頭，藉由數位平台(digital platform)與大型語言模型（LLMs）正向人類施以高壓、高量的內容，這些內容多以連續的、負面的「黑暗社群媒體材料」（dark social media material）形式呈現，目的是為了從中不斷榨取用戶注意力並轉為商品化，迫使人們的注意力集中在可被轉售的「泡沫」（fro

th），並透過拍賣機制販售給廣告商與政治操作者。然而，石油壓裂會導致地質不穩定和地表污染，人類壓裂則容易造成深刻的社會秩序混亂或政治結構的動態，例如社會孤立化（siloing）、公共討論失衡及政治不穩定。

而人工智慧(AI)亦扮演人類壓裂關鍵的角色。AI並非具有意識的實體，但其模擬人類大部分行為的特性，無疑提供了探究人類意識的新契機，AI系統透過不斷演進的語言模型、演算法加速了將人類行為轉化為可貨幣化的商業利益。

（三）注意力行動主義及庇護

針對上述挑戰，B教授以「注意力行動主義」（attention activism）作為回應框架，並提出「**注意力解放運動**」(attention liberation)。其核心在於建構新的制度與社會性庇護（sanctuary），以保護人類免於無止境的數據壓榨。其中注意力行動主義的三大支柱如下：

1. **學習（Study）**：重新審視注意力作為數據資源的歷史與社會意涵。本身被視為一種專注的、存在主義的實踐（existential practice），並非強調自動化的「搜尋」（search）不同；學習將自身與主題融合，從而成為不同的人，例如B教授於紐約創立了「激進發明之奮鬥者學校」（Struggler School of Radical Invention, SoRA），並強調注意力是當前社會之關鍵問題，而教育必須將豐富的注意力視為自由的必要條件。

2. **組織**（Organizing）：匯聚跨國行動社群，形成集體力量，其中涉及透過共享的創造性、心理學和政治策略，共同抵抗注意力被惡意榨取。

3. **庇護**（Centering/Sanctuary）：建立免於人類壓裂侵害的安全空間，此概念與隱私保護的概念息息相關，例如庇護空間(sanctuary space)並非僅僅是物理性的隔離或躲藏，而應視為一種能夠提供「存取與探索」機會的環境，例如圖書館、學校與博物館，均可作為避免數據剝削的實體避難所。

（四）政策整合及行動呼籲

B教授回顧美國法學家Louis Brandeis對隱私權的早期論述。最初**之所以關注隱私權，正是防止商業濫用與形象剝削**。例如，一名女性的照片曾未經允許被廣泛印製於麵粉袋上，引發公眾對商業侵害的反思。

他強調注意力解放運動應與現有的隱私保護行動有所鏈結，全球每人平均一天花費約9至11小時於數位螢幕前，逐漸成為「注意力主體」（homo attentivus）。倘缺乏有效的數據治理與隱私保護，人類自由將被「注意力政治學」（attentional politics）所劫持。

他疾呼現今我們處在一個緊張時刻(tensity)，如同19世紀工業革命時期，勞工階級從被貶低的勞動力轉變為有政治權力的行動者的歷史轉折點，並呼籲在場隱私專業人士必須正視兩大核心問題：

1. 如何透過隱私政策與法規，支持「庇護空間」的建構與維護？

2. 如何讓關注注意力政治的行動主義社群，與隱私專業工作相互支援與擴展？

最後，B教授提及，長期致力於注意力研究的非營利組織「注意力之友」(The Friends of Attention)，預計於2026年一月發布《注意力解放》宣言（Attensity!: A Manifesto of the Attention Liberation Movement)。該宣言強調，為了有效應對「注意力經濟」所帶來的剝削與社會性風險，隱私保護措施或政策必須與公民社會的草根行動相互整合協調，方能建構完整的社會機制。

場次五（Panel Session 5）：代理式人工智慧與隱私（Agentic AI and Privacy）

主持人及現場與談嘉賓，由左至右分別為Yong Lim、John Edwards、Jules Polonetsky、Kate Charlet、Yoochul Kim

主持人：Yong Lim（韓國首爾大學教授，Professor, Seoul National University）

與談人：

- John Edwards（英國資訊委員辦公室辦公室資訊專員，Information Commissioner, ICO, UK）
- Jules Polonetsky（未來隱私論壇執行長，Chief Executive Officer, Future of Privacy Forum）

- Kate Charlet（Google 全球隱私、安全與保障總監，Global Director for Privacy, Safety, and Security, Google LLC）
- Yoochul Kim（LG AI 研究中心策略部主管，Head of Strategy Unit, LG AI Research）

隨著人工智慧技術從內容生成（Generative AI）快速演進至主動式代理（Agentic AI），其影響力已不僅止於資訊的產出，更擴及任務的自主執行。因此，深入了解此一技術演進對現行隱私權框架帶來的衝擊、產業的應對策略，以及未來的監管方向，對於我國制定前瞻性的數位政策與人工智慧治理框架至關重要。以下為本場次討論重點：

（一）技術演進的關鍵轉向：從生成式AI到主動式AI的範式變化

主持人L教授指出，生成式AI（Generative AI）代表的是「內容創造」時代，而主動式AI則標誌著人工智慧邁入「自主執行」的新階段。其不僅能生成文字、圖像或程式碼，更能在理解上下文與任務目的後，自主規劃並執行行動，成為數位環境中能「替人行動」的智能代理。

Google C總監將其比喻為從「內容引擎」進化為「互動式專案經理」。前者著重於回應使用者指令、生成成果；後者則能感知環境、推理決策，並以最少人為干預自主完成任務。此種轉變則標誌著AI不再只是輔助工具，而是具備行為能力的「行動主體」（active agent），能主動協調多個系統、平台與API，以執行複雜任務。

與談者一致指出，主動式AI具備三項核心能力：其一是推理與規劃（Reasoning & Planning），能夠分解高層次任務並設計執行

步驟；其二是跨系統操作（Cross-system Operation），可整合外部工具與平台進行動態互動；其三是自主執行（Autonomous Execution），能依情境調整策略、持續運作。這些能力的結合，使得AI不再受限於單一平台的邏輯，而具備跨域的「決策與行動能力」，進一步改變了人與機器、使用者與資料之間的基本關係。

然而，這種自主性也打破了現行隱私治理的邏輯假設。過去的法制以「使用者主動提供資料、服務被動接收」為基礎，而主動式AI反其道而行之，能「自行決定」蒐集、整合與使用資料。這正是座談會全程討論的核心問題：當AI具備「代理」能力時，傳統的同意制度、控制架構與法律責任歸屬，是否仍然適用？

（二）隱私的雙面刃：自主性帶來的風險與潛在機遇

與談者普遍認為，主動式AI的自主運作模式是一把雙面刃。一方面，它可能顯著放大資料蒐集與控制權不對稱；另一方面，它也為「技術強化隱私」（privacy-enhancing by design）開啟新契機。座談中的多位專家均以「隱私風險的再定義」為焦點，嘗試從動態系統的視角重新理解資料保護。

首先，AI代理的動態資料蒐集能力帶來了前所未有的風險。與傳統應用在特定平台上被動收集使用者資料不同，主動式AI能即時、跨平台地存取多個資料來源，包括行事曆、郵件、定位資訊、社群資料等，以達成任務。這意味著使用者可能在未察覺的情況下，暴露出大量敏感資訊。這種「非預期性資料流」挑戰了現行隱私法以「明確同意」為核心的制度基礎，也使「目的限制」原則（Purpose Lim

itation）難以落實，因為代理在執行單一目標時可能跨越多個不同法律脈絡的資料場景。

其次，人類代理權（human agency）與知情同意機制的侵蝕成為重要議題。現行的同意框架假設使用者可逐步、明確地對單一服務行為進行授權，但當AI能同時操作多個網站（如自動訂機票、訂房、安排交通）時，逐次點擊的模式將失效。C總監指出，這不僅是技術挑戰，更是「人類主導權的結構性削弱」。若使用者無法再有效掌控自身資料的流向，整個隱私體系將形同虛設。

第三，責任歸屬的模糊化是產業與監管者共同面臨的棘手問題。主動式AI的決策鏈條涉及模型開發者、服務平台、第三方API及使用者端應用，一旦發生資料外洩或錯誤決策，誰應負責？未來隱私論壇P執行長指出，在當前的供應鏈架構下，資料控制者（controller）與處理者（processor）界線愈發模糊，這使得監管的可執行性大打折扣。

儘管如此，座談也展現了技術導向的隱私強化新契機。主持人L教授引述討論指出，若設計得當，AI代理未必是風險製造者，反而可能成為「個人隱私守護者」（personal privacy guardian）。例如，它可被編程為在互動過程中自動執行資料最小化原則（Data Minimization），僅傳遞完成任務所需之最小資訊。此外，Google代表C總監分享，部分主動式AI已被應用於網路安全領域，能主動偵測與修補潛在漏洞，預防資料外洩。這種「主動防護式隱私治理」（proactive privacy governance）將可能重塑數據安全的基本思維。

（三）治理的新路徑：從設計思維到原則性監管的整合架構

在治理層面，與談者普遍認同應「以既有法制為基礎、以技術創新為助力」，而非另起新法。產業與監管雙方均強調，現行資料保護原則在精神上仍適用於主動式AI，但需在實務層面進行延展與調整。故而，本場次之產業界代表提出了四項主要策略：

首先是「**隱私設計**」（Privacy by Design）。這是將隱私視為技術開發的前提條件，而非事後補救。企業應在模型訓練、任務規劃、授權管理等階段即納入資料治理機制，確保隱私防護與系統運作並行。LG研究中心的K部門主管指出，韓國企業已開始建立「隱私評估模板」（Privacy Assessment Templates），作為開發初期的必備審查程序。

其次是「**技術性保障措施**」（Technical Safeguards）。例如以合成資料（Synthetic Data）或假名化（Pseudonymization）取代真實資料進行模型訓練，可在降低風險的同時維持模型效能。這類技術被視為兼顧創新與隱私的中介方案。

第三是「**透明度與可解釋性**」（Transparency & Explainability）。AI代理應具備向使用者說明其決策邏輯的能力，讓使用者能理解其行為依據與判斷過程，即便不公開所有技術細節，也需確保行動的「可預測性」。

最後是「**權限最小化原則**」（Least Authority Principle）。AI代理的操作權限應嚴格限定於完成任務所需之範圍，例如行事曆管理代理不應被授權存取財務資料。這種最小授權的設計有助於防止資料外洩與權限濫用。

在監管端，英國資訊委員辦公室（ICO）E專員強調，主動式AI雖具創新性，但仍屬「技術演進」（evolutionary）而非「法律真空」（lawless lacuna）。他駁斥媒體對ChatGPT出現後「監管失效」的誇張敘事，並指出《一般資料保護規則》（GDPR）等既有框架在原則層面仍完全適用。其核心應對策略可歸納為三點：

一是維持原則性監管（Principle-based Regulation）。資料最小化、目的限制、準確性與可追溯性等原則仍為審查主動式AI合規性的核心依據，重點在於調整實施方式而非另立新法。

二是促進產業協作與政策對話(Collaborative Co-regulation)。監管機構應建立「創新沙盒」（Regulatory Sandbox）與「合規諮詢服務」（Innovation Advice Service），鼓勵企業於開發初期即與監管者互動，降低創新不確定性。

三是確保人類代理權（Human Agency）與責任可追溯（Accountability）。E專員特別指出：「透明度是核心。我們必須確保在便利與自動化之間，人類仍然是掌控者。」

在政策層面，主持人L教授總結指出，未來的治理方向應包括三項關鍵轉型：

第一，從靜態規範走向動態評估（From Static Regulation to Dynamic Assessment），即建立能隨AI自主行為持續監控與調整的合規系統；

第二，從單一監管者走向多方協作（From Single Regulator to Multi-Stakeholder Governance），強化政府、產業、研究與公民社群之間的共同監理；

第三，從法遵導向走向倫理導向（From Compliance to Ethics-driven Governance），將人類價值與社會信任納入 AI 發展的核心指導原則。

綜觀整場討論，與談者達成高度共識：主動式AI不應被視為顛覆現有法制的「外來物」，而是既有監管框架的新挑戰。現行隱私法所依循的核心價值—透明、問責、資料最小化與個人主體性—仍具普遍適用性，但其具體實踐方式必須轉向動態、持續與協作型的治理模式。主動式AI的出現，使資料治理進入一個以「自律互動、風險可控」為特徵的新時代。其真正挑戰不在於技術本身，而在於能否建立一套兼顧創新驅動與權利保障的治理生態。此一議題，亦將成為未來全球隱私與AI政策對話的核心主軸。

場次六（Panel Session 6）：支持人工智慧創新的機制與政策工具（Mechanisms and Policy Instrucments to Support AI Innovation）

主持人及現場與談嘉賓，由左至右分別為J. Trevor Hughes、Des Hogan、Stefano Fratta、Stefano Fratta、Yeonjea Kim

主持人：J. Trevor Hughes（國際隱私專業人員協會總裁兼執行長，President and CEO, IAPP）

與談人：

- Bertrand du Marais（法國國家資訊與自由委員會國際事務專員，International Affairs Commissioner, CNIL, France）
- Des Hogan(愛爾蘭資料保護委員會委員,Commissioner,DPC,Ireland）
- Stefano Fratta（Meta 公司副總裁，Vice President, Meta）

- Yeonjea Kim（Kakao公司隱私保護長，Head of Privacy, Kakao Corp.）

本場次座談圍繞著AI時代下監管如何與創新同行，會談中之討論之重點如下：

（一）監管創新的必要性與多樣化途徑

面對AI技術的快速迭代，與會者一致認為監管思維必須跳脫傳統的執法框架。主持人以蜘蛛網比喻，說明單一、僵化的監管模式已無法應對當前的複雜性。法國國家資訊與自由委員會國際事務M專員說明在法治基礎上，DPA應扮演市場教育者、諮詢者與合作夥伴等多重角色，透過公眾諮詢、強化支援服務等工具，將監管從被動的限制轉為主動的引導。愛爾蘭DPC則以實際案例說明監管者如何掌握好何時溝通、何時執法，並聯合其他監管機構共同塑造一個可預測、一致的監管環境，最終目標是為創新建立穩固的信任基礎。

（二）諮詢機制（監管沙盒）的價值與現實困境

監管沙盒與事前審查等諮詢機制亦是本場次討論重點。對於產業界而言，沙盒之最大價值在於成為對抗「法律不確定性」的解方。Meta的專家透過在韓國、新加坡、英國的具體合作案例，說明這些機制如何幫助企業找到合規的可行性。Kakao公司K隱私保護長也肯定其對於降低新創服務市場風險的作用。不過，現狀仍存在許多挑戰：全球企業正面臨「規模化」與「碎片化」兩大痛點，一方面企業難以與全球數百個監管機構逐一進行深度溝通，另一方面，單一國家的合規認可並無法保證全球通行，使這類機制的效益不彰。

（三）從外部監督到內部治理：邁向自律的未來

會議當中討論到，監管的終極目標應是催生企業內部的治理能力。與談人提出建議認為：監管資源應集中用於應對真正的「高風險」場景，而對於廣泛的AI應用，則應大力推動「自我規管」，其分享了Kakao內部從原則、風險管理到治理架構的完整實踐，並呼籲監管機構轉向扮演賦能者 (enabler)的角色，例如提供隱私增強技術(PETs) 或基礎資料集等公共財，來幫助企業建立自身的防護網。也就是說，當企業將保護使用者作為核心價值內化於產品設計與公司治理中，外部監管的壓力自然會轉化為創新的動力。

主題演講四（Keynote 4）

OpenAI 首席策略長 Jason Kwon演講

本場次由**OpenAI首席策略長Jason Kwon（Chief Strategy Officer）**主講。K執行長首先闡明，OpenAI的根本使命在於確保人工智慧之發展能惠及全人類，而此一使命必須以「信任」為核心。信任的建立，不能僅止於形式化的法規遵循，而應透過具體行動予以實踐。為此，OpenAI已推出臨時對話機制，使使用者得以自主決定其資料是否可用於模型訓練；並明確承諾不將企業客戶之數據用於訓練用途。此外，公司亦設立自助式隱私門戶，便利公眾查詢相關政策，並得依需求提出刪除個人資訊之請求。K執行長強調，OpenAI在此過程中持續吸收各國監管機構之意見，據以優化制度，以期臻於完善。

其後，K執行長論及人工智慧與隱私之關係，認為AI不僅可能引發隱憂，亦能成為維護隱私之助力。如OpenAI已成功研發隱私過濾器，以減少模型

訓練時對個人數據之依賴，且其效能優於現有商業工具。公司計畫於2026年將此技術開源，期望透過全球開發者的共同努力，全面提升隱私保護水準。除技術革新之外，OpenAI亦推動民主價值，嘗試透過自然語言對話，協助使用者迅速理解並行使隱私權益；同時著手建構家長監控工具，以確保青少年在使用AI時的安全與健康。

關於未來之挑戰，K執行長提出兩項重要議題。其一，AI系統正逐漸演進為能代表人類行動之智能代理，然**其設計應以強化人類自主性為宗旨，而非取而代之**。因此，隱私必須成為信任的核心，並於系統中設置安全護欄，**讓使用者得以掌握代理行為的主導權**。其二，針對「AI特權」問題，K執行長指出，現行法律制度尚不足以應對人類與AI之私人對話，致使其恐淪為訴訟、傳票或調查之對象。因而，**亟需檢討與修訂法律規範，並輔以技術方案，以確保個人自主與選擇權**。

最後，K執行長強調，隱私之本質不僅止於技術或監管問題，而在於人性。它體現尊嚴、自主與對個體的尊重，並構成人類社會持續進步的根基。

場次七（Panel Session 7）：促進跨境資料傳輸的互通性（Enhancing Interoperability in Cross-Border Data Transfers）

主持人及現場與談嘉賓，由左至右分別為Philippe Dufresne、Christopher Kuner、Immaculate Kassait、Yuji Asai、Alexander Joel

主持人：Philippe Dufresne（加拿大英屬哥倫比亞省資訊及隱私專員，Privacy Commissioner, Commissioner, OIPC, BC Canada）

與談人：

- Christopher Kuner（丹麥哥本哈根大學教授，Professor,University of Copenhagen，主講人）
- Immaculate Kassait（肯亞資料保護委員辦公室，Commissioner,ODPC, Kenya）

- Yuji Asai(日本個人資訊保護委員會專員，Commissioner,PPC,Japan)
- Alexander Joel（美國華盛頓美利堅大學法學院教授，Professor, American University’s Washington College of Law）

本場次探討了AI時代下跨境資料傳輸的複雜性，與談者的觀點重點摘錄如下：

（一）地緣政治下的法治基礎

討論當中，Kuner教授認為，法治是個資保護存在的前提，任何對民主制度的侵蝕都會動搖資料保護的根基。Joel亦認同該觀點，從國家安全的角度認為AI的競賽實則是民主與威權兩種價值體系的對抗，民主國家間的團結與互信是重要的關鍵。

（二）互通性工具的挑戰與創新

與談者普遍認為，現有的傳輸工具如適足性認定、標準契約條款等，面臨著複雜、高成本且難以規模化的困境。Immaculate Kassait專員描述了非洲企業面對多國破碎法規時是一種監管夢魘(regulatory nightmare)。對此，討論當中提及的解決方式例如，發展更具彈性的「轉接頭」機制，銜接各國不同的法規範差異，透過OECD政府資料存取宣言等方式建立共同原則等；或是為中小企業量身打造簡化的行為準則或認證；此外，也有專家認為宜建立如全球CBPR這樣更具互通性的體系，將「信任」機制化。

（三）資料保護主管機關的角色再定位

會議中的專家均同意DPA的角色正在演進。Kassait專員指出對於產業界與發展中國家而言，DPA不應只是執法者，更應是促進經濟發展與創新的促進者。而Kuner教授則賦予DPA更高的期許，認為其應成為民主價值的捍衛者。這顯示DPA未來的挑戰，是在扮演監管者、促進者與捍衛者等多重角色間取得平衡。

平行論壇2-A（Parallel Session 2-A）：青少年隱私：實務操作（Youth Privacy: Mechanics）

主持人與現場與談嘉賓，由左至右分別為Michael Harvey、Sanghee Park、Leanda Barrington-Leach、Elaine Fox、Hilary Ware

主持人：Michael Harvey（加拿大英屬哥倫比亞省資訊及隱私專員，Commissioner, OIPC, BC Canada）

致詞人：Melissa Holyoak（美國聯邦貿易委員會專員，Commissioner, FTC, USA）

與談人：

- Sanghee Park（韓國個人資料保護委員會專員，Commissioner, PIPC, Korea）

- Leanda Barrington-Leach（5Rights 基金會執行董事，Executive Director, 5Rights Foundation）
- Elaine Fox（TikTok 歐洲隱私負責人，Head of Privacy, Europe, TikTok）
- Hilary Ware（Apple 公司全球隱私與線上安全主管，Global Head of Privacy and Online Safety, Apple Inc.）

本場會議由監管與產業專家共同討論，圍繞著兒少數位隱私的核心困境。各方觀點可歸納如下：

（一）年齡驗證的技術兩難

年齡驗證(Age Assurance)是本次會議的焦點。美國FTC的H專員表示，執法機構正積極透過政策誘因，推動業界採用更可靠的年齡驗證技術，以取代漏洞百出的自我宣告機制。然而，Apple的隱私與線上安全W主管警告，現行破碎化的法規，正迫使平台為了合規而進行更精細、更具侵擾性的用戶年齡追蹤，這與隱私保護的初衷背道而馳。TikTok歐洲隱私F負責人也指出，全球對何種技術（如數位錢包或臉部年齡估算）是最佳方案尚未形成共識，且任何技術都必須在設計之初就將隱私保護內建其中。

（二）責任的再分配：從使用者自保到系統性變革

誰該為孩子的網路安全負責？5Rights基金會執行B董事認為責任必須從兒童與家長身上，轉移到平台與服務提供者。她認為，要求使用者在一個為營利設計的環境中具備數位素養，是不公平且無效的。韓國PIPC的P專員也提到，透過立法來規範企業如何處理兒少

個資，正是將責任制度化。兩位業界代表強調其已提供多樣的家長控制工具，但公民社會的觀點顯然認為，將選擇權交給使用者是不夠的，應該要預設一個安全的數位環境。

（三）監管碎片化的反作用力：善意的初衷如何導致隱私惡果

業界代表指出全球各地各自為政的監管模式是一個議題，例如不同國家設定的年齡門檻（例如13、14、16歲）和過度概括的合規要求，會導致三項風險：一是違反資料最小化（data minimization）原則，迫使無關的App也需獲取年齡資訊；二是剝奪了家長根據孩子成熟度進行判斷的自主權(parental autonomy)；三是為了應對複雜的法規，平台不得不建立更精細的用戶剖析系統，反而增加了隱私風險。

平行論壇2-B（Parallel Session 2-B）：資料保護的救濟與互通性：消費者觀點（由亞太數位消費者對話主導）（Redress and Interoperability of Data Protection: The Consumer Perspective (led by the Asia Pacific Digital Consumer Dialogue）

主持人及現場與談嘉賓，由左至右分別為Amy Kato、Guido Scorza、Hiroshi Miyashita、Javier Ruiz Diaz、Natascha Gerlach、ByoungIl Oh

主持人：Amy Kato（日本消費者組織代表，Consumers Japan）

與談人：

- Guido Scorza（義大利個人資料保護機關隱私專員，Commissioner, GPDP ,Italy）
- Hiroshi Miyashita（日本中央大學政策研究學部教授，Professor, Faculty of Policy Studies at Chuo University）

- Javier Ruiz Diaz（亞太數位消費者對話顧問，Advisor, Asia-Pacific Digital Consumer Dialogue）
- Natascha Gerlach（資訊政策領導中心隱私政策總監，Director of Privacy Policy for the Center of Information Policy Leadership）
- ByoungIl Oh（韓國進步網路 Jinbonet 總裁，President, Korean Progressive Network Jinbonet）

本場平行論壇旨在探討在全球化資料流動的背景下，國際資料治理機制所面臨的執法與救濟困境，並集結多位跨領域專家，從執法、學術、公民社會與業界角度提出見解，重點摘要如下：

（一）法律與現實之間的差距：跨境執法的困境

義大利個人資料保護機關隱私S專員以義大利對Clearview AI的執法案[10]為例，說明當代的資料保護正面臨一個核心困境，亦即法律規定與實際執行效果之間存在著巨大的差距：

美國公司Clearview AI被指控非法蒐集全球數百萬，甚至數十億人的臉部照片，並從中提取生物辨識識別碼，用於提供 AI 驅動的人臉識別服務。義大利資料保護局在收到大量公民投訴後，於2021年展開調查，認為該公司非法蒐集、處理義大利公民的生物辨識資料，義大利資料保護局於2022年2月正式作出裁決，命令Clearview

[10] 義大利資料保護局（Garante）於2022年2月對Clearview AI開立2000萬歐元罰款，指控其違反GDPR非法透過網路抓取蒐集義大利人士生物特徵與地理位置資料（建置逾100億張臉部資料庫），並缺乏合法依據、透明資訊與歐盟代表，同時命令停止處理、刪除相關資料並回應資料主體權利請求。Garante per la protezione dei dati personali. (2022, February 10). Facial recognition: Italian SA fines Clearview AI EUR 20 million. https://www.edpb.europa.eu/news/nationalnews/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en

AI刪除所有與義大利資料主體相關的所有資料，停止在義大利境內的生物資料收集與處理，並處以2,000萬歐元的巨額罰款。

Clearview AI在收到裁決通知後，該公司隨即「消失」，既未對裁決提起上訴，也未支付任何罰款，且未回應義大利當局發出的後續要求，亦未確認義大利境內資料是否確實刪除，義大利資料保護局發出的多封後續通知均未獲回應。

上開執法過程顯示國際合作的嚴重不足，儘管歐盟與美國之間存在《隱私盾》（Privacy Framework）等機制，但義大利與美國之間缺乏關於此類行政命令的通知或強制執行的雙邊協議或公約，導致義大利當局無法強制執行裁決。S專員指出此問題不僅限於義大利與美國之間，義大利在與瑞士和中國的跨境執法中也遇到相同的執行困境。

Clearview AI案例證明，即便有GDPR等全球性法律框架，執法和權利落實仍面臨現實困境。在缺乏有效的國際執法合作機制下，資料保護機構難以確保居住在國內的資料主體之權利能被有效實現，對消費者而言，最重要的是其隱私權能夠得到有效、實質的保護，而非僅是法律條文規定。

故而，針對跨境執法機制的不足，S專員提出以下幾點可解決的方向。首先，S專員回顧歷史中世紀「商人法」（lex mercatoria）的誕生，正是為了解決當時世界各地商業活動中共同立法的需求與執行問題。鑒於今日全球社會中資料自由流動的特性，**世界需要一部新的、類似中世紀商法體系的「資料商人法」**（Data Lex Mercat

oria），用於規範全球資料流動，確保全球範圍內真正的法律確定性，從根本上解決各國資料保護法規在跨境執法上的隔閡與衝突。

再來，需塑造隱私文化，讓人們「愛上隱私權」(fall in love with privacy)。隱私保護重心應從單純的法律制定轉向塑造市場文化與提升用戶體驗，其核心觀點是：「尊重隱私不是競爭障礙，而是成功的驅動力」，資料保護機構必須竭盡所能，提升大眾對隱私價值的認知。**企業為了獲得市場信任與競爭力，將會自發地遵守規則，而非僅僅是為了避免罰款。**

最後是提升隱私的「可用性」（Usability）。S專員提出了一個創新的比喻，資料保護應被設計成像數位服務一樣易於使用的一種「產品或服務」，因為資料保護不如Facebook、TikTok 或ChatGPT等數位服務容易使用，在現今的數位世界中，用戶只需「輕輕一點」（one tap）就會失去機密性，然而，若想恢復權益或獲得保護，卻往往需要耗費數年時間與高昂的金錢成本。因此，資料保護機構應將重點從原則轉向工具，使資料保護具備直觀的操作界面，簡化資料主體行使權利的流程，讓資料主體能夠透過「一鍵操作」，就能夠行使權利並獲得有效的保護，大幅降低維權的門檻。當隱私權變得如同受歡迎的數位產品一樣具有「可用性」時，民眾將會主動推動行業去尊重隱私，將其作為在市場上取得成功的方式。屆時，對國際執法的依賴性將會相對降低，因為市場力量將會促使企業自願遵守規則。

（二）全球資料傳輸制度的多層架構與跨境複雜性

日本中央大學政策研究學部M教授首則將全球資料傳輸機制分為四個層次，從最軟性的合作性框架，到具有強制法律效力的制度，並說明這些機制的法律約束力和運作特性的相同：

1、最軟性方法（Softest Approach）：此類機制以資訊交換與合作為主，旨在建立跨國互信，但缺乏強制法律約束力。典型例子包括 OECD 隱私框架以及全球隱私執法網絡（GPEN）。OECD 隱私框架自 2007 年就已啟動資訊交換，並已有全球超過 50 個參與機構。

2、區域性橋接（Regional Bridges）：此主要在特定地理或經濟區域內建立共通規則，試圖達成區域內互通性。代表性制度包括 APEC 跨境隱私規則（Cross-Border Privacy Rules, CBPRs）、歐盟 BCRs（Binding Corporate Rules）。Miyashita 教授也指出，儘管業界和學術界在2013年開始討論如何使APEC CBPRs 與 EU BCRs 之間具有互操作性，然而2014年的研究指出，這些區域性機制在某些關鍵要素上仍不相容，顯示區域橋接仍充滿挑戰。

3、具法律約束力的機制（Legally Binding Mechanism）：以歐盟的「適足性認定」（Adequacy Decisions）為例， 此類機制透過國家層級的主管機關認定，為資料傳輸建立最強大的法律保障與權利基礎。目前歐盟已做出了 16 個適足性認定決定，允許個人資料自由流動至被認定具備充分保護的國家或區域。

4、最強健的跨境救濟機制：歐盟「一站式服務」（One-Stop Shop Mechanism） Miyashita 教授認為，在所有機制中，歐盟的「一

站式服務」（OSS）機制，是目前他所理解中，法律約束力最強大、最穩健的跨境救濟類型。它允許企業與主管機關在單一國家進行協調，簡化跨境資料傳輸與監管程序。

M教授指出在上開全球資料傳輸機制架構下，由於不同的傳輸管道並存，顯示跨境傳輸的複雜性，並舉例若某公司須將個人數據出口到不同的第三國時，必須根據目的地國家的情況，進行個別的資料傳輸影響評估（Data Transfer Impact Assessment, DTIA）。如果出口到歐盟國家，可依靠適足性認定；出口到美國或北美國家，則可能需符合OECD標準；但若出口到隱私立法不成熟的東亞或南亞國家，企業可能必須依賴APEC CBPRs，或為每次傳輸針對每個目的地進行個別的資料傳輸影響評估，大大增加了跨國企業在資料傳輸上的合規成本與難度。

進一步而言，全球在消費者救濟思維上呈現兩極化：歐盟採「風險導向(Risk-based Approach)」模式，無需證明實際損害已經發生，只要證明存在資料被濫用或非法存取的風險，法院或監管機構即可介入並提供救濟。重視潛在風險即可啟動監管，以防患未然；美國則維持「損害導向(Harm-based Approach)」思維，核心理念為「沒有具體傷害，就沒有訴訟資格」（No concrete harm, no standing)。原告必須證明遭受了具體的、可衡量的損害(Concrete Harm)，才能獲得進入訴訟程序的資格。強調具體損害證明與訴訟資格。。

M教授最後指出，全球資料傳輸機制與消費者救濟模式密切相關：

1、不同國家或區域的資料傳輸機制影響企業的合規策略。

2、消費者救濟的門檻受到法律模式差異的影響:歐盟的風險導向降低了訴訟障礙，而美國的損害導向則提高了救濟門檻。

3、對跨國公司而言，了解各種制度層級和救濟模式，並進行風險評估與影響分析，是全球數據治理的重要課題。

（三）韓國救濟制度的存在與失靈

韓國進步網路 Jinbonet 0總裁以自身在韓國公民組織的實務經驗分享作為公民社會代表的親身經歷。為了評估南韓救濟機制是否運作正常，Jinbonet等民間組織在2020年針對韓國三大電信公司SKT、KT和LG U+提出要求授予資料主體個人資訊訪問權，並停止處理其資訊以用於科學研究目的。三家公司均拒絕部分資訊存取請求，並停止相關處理。組織因此分別採取了三種代表性的救濟程序，結果顯示這些途徑皆有其侷限性：

1、個人資訊爭議調解 (Dispute Mediation)：

針對KT電信提請的調解案，結果顯示爭議調解委員會是一個相對迅速且有效的機制。在申請後約四個月，委員會就做出了有利於消費者的調解決定，命令保障存取權並停止處理個人資訊，且KT接受了此決定。然而，該機制存在根本的缺陷，只要其中一方拒絕接受調解方案，整個機制便會立刻失靈。例如另一起針對Meta(Facebook)未經授權向第三方提供用戶資訊的事件，Jinbonet組織召集181名用戶提出集體爭議調解，儘管調解委員會提出每位申請人可獲30萬韓元賠償並可查詢第三方身份的方案，但由於Meta拒絕接受調解，調解隨即失效，迫使受害者只能轉向成本更高、耗時更長的訴訟途徑。

2、個人資訊侵權舉報（Infringement Report)中心：

針對LG U+電信的侵權舉報案，耗費了超過一年（直到2022年7月）才收到回覆，該中心的回覆僅簡單指出LG U+已在其網站上提供相關資訊，不構成違法。此行政救濟途徑耗時過長，且回應內容僅為形式性的指導，無法提供實質救濟。侵權舉報中心雖然理論上是最容易使用的途徑，但實務上效率低下，未能有效保障用戶權利。

3、法律訴訟（Lawsuit)：

針對SKT電信的訴訟案，雖然在一審和上訴法院中均均判決使用者勝訴，認為用戶可以要求SKT停止將其個資用於科學研究的匿名化處理。但案件在今年7月案件被最高法院推翻並發回重審，最高法院認為將個人資訊「去識別化」（匿名化）用於科學研究不同於個人資訊處理。訴訟儘管是資料主體尋求救濟的重要手段，但在面對大型企業時，訴訟門檻極高，且最終可能因司法判決而導致不利結果。訴訟被證明是耗時、成本高昂且充滿不確定性的救濟手段。

藉由以上資訊，O總裁發現，在個人資訊洩露等受害者眾多但個人損害金額往往很小的案件中，例如最近涉及超過2,000萬筆資料的SKT用戶資訊洩露事件，數萬名用戶不得不提起損害賠償訴訟，但韓國缺乏針對個資侵權的真正集體訴訟制度使他們難以獲得有效賠償，其原因有二：韓國沒有針對個人資訊侵權的集體訴訟制度，使得集體維權的成本非常高，再來，儘管韓國《個人資訊保護法》設有代表人訴訟制度，允許符合特定標準的消費者組織代表受害者提起

訴訟，但該制度設計只能用於請求法院下令停止侵權行為，不允許請求損害賠償，代表人訴訟制度實際上是名存實亡，至今尚未有根據《個人資訊保護法》提起的損害賠償代表訴訟的案例。

O總裁指出儘管韓國已建立了法律框架，但在為資料主體提供有效和及時救濟方面仍有諸多限制。為了有效保障廣大受害者的權益，他主張韓國必須優先推動兩項關鍵改革：

1、引入真正的集體訴訟制度，簡化受害者索賠流程，使大規模個資侵權案件受害者能夠就個人資訊侵權案件提起損害賠償訴訟，降低資料主體的救濟成本。

2、增加個人資訊侵權舉報中心的人員和能力，以確保用戶能夠獲得迅速和有效的行政救濟。

（四）全球資料跨境流動與互操作性的現況Javier Ruiz Diaz（亞太數位消費者對話顧問）

亞太數位消費者對話D顧問首先說明了「互操作性」（Interoperability)的理念是承認各國永遠無法在所有事情上達成完全一致，因此需要尋求兼容的機制。然而目前國際間在討論資料跨境流動的「互操作性」時，往往過度聚焦於法律機制、規則和保障措施等前端工具對接上，而忽略了後端的資料主體的權力、監督、執法與救濟，而這正是導致消費者普遍不信任跨境資料傳輸的根本原因，消費者擔心當他們的資料傳輸到另一個國家並被用於某些目的時，他們將失去更多對資料的控制，且許多在國內可能遇到的問題，在資料跨境傳輸後將變得更加複雜。

D顧問強調，資料跨境流動涉及多方利害關係人，尤其是企業與消費者，企業與消費者在跨境資料傳輸問題上有著根本性的差異，企業追求的是一份「合法化」資料傳輸的文件，方便繼續業務；消費者關注的是在資料被合法化之後，如果出現問題，如何得到實際補救。這種對「合規」與「實際救濟」的巨大關注落差，是當前資料治理面臨的核心矛盾。

D顧問強調適足性認定本身並非一種救濟機制，而只是促成資料合法跨境傳輸提供合法性基礎的前置工具。真正的問題仍可能在資料傳輸至接收國之後才發生，屆時消費者仍需面對跨國求償、執法困難等以下挑戰：

1、 **訴訟資格（Standing）問題**：由於各國對於訴訟資格的要求不同，特別是如前述美國採取的「基於損害」(Harm-based)模式，消費者可能因無法證明自己遭受了具體損害而被拒於法院門外。

2、**高昂的法律成本與財務風險**：跨國訴訟費用極高，對個人而言難以承擔。在許多國家，一旦上法庭，法律成本和財務風險都是一個巨大的問題。

3、**語言障礙**(Language Barriers)：聯繫外國監管機構或法院時，語言成為重大障礙，即便歐盟的「一站式服務」（One-Stop Shop）也可能因文件在歐盟內部德語和英語之間的翻譯過程，實際上可能削弱了「一站式服務」的效率。

4、**執法機構權力有限**：如義大利DPA案例所示，即使是國家級資料保護機構，在跨境執法時也可能面臨權力受限的困境。

5、**集體訴訟障礙**：在集體訴訟方面，消費者也面臨著包括缺乏「選擇退出（opt-out）」機制、資訊不透明、法律成本高昂等問題。

為解決以上問題，D顧問援引聯合國的《消費者保護指導方針》，該指南要求提供有效的消費者爭議解決與救濟，強調一個有效的救濟機制，不僅必須能夠為個案受害者討回公道、提供實際的補償，更必須具備嚇阻未來不當行為的功能。Diaz呼籲國際間在制定互操作性政策時，應重視「執法與救濟」的落實，而非僅停留在法律文件或聲明層面，否則消費者對跨境資料流動的不信任將持續存在，並成為全球資料經濟發展中的核心障礙。

（五）從事後救濟（The After）轉向事前預防（The Before）

資訊政策領導中心CIPL G總監從業界與實務運作的角度進行說明，首先呼應義大利S專員的觀點，指出**有效的救濟（effective redress）是建立信任的基石**。G總監也強調預防的重要性，若一切重心僅放在「事後補救」（the after），往往意味著損害已經發生，因此更應將焦點前移，著眼於「事前預防」（the before）。因此，**現代資料保護應從單純的「救濟導向」轉向「預防導向」**。預防的核心在於強化組織的「問責制」（accountability），並提高對消費者的透明度（transparency），讓企業能在問題發生前就建立完善的防線與回應機制。一個成熟的隱私生態系統，應該是讓救濟的需求降到最低的系統。

GDPR等現代隱私法規中所要求的透明度義務，確實大幅提升了民眾對其個人資料如何被使用的意識，民眾對個人資料的使用方式愈加關注，也更清楚如何主張自身權利，導致各國監管機關收到的

申訴量顯著上升。然而，同時也促使企業正面應對挑戰，積極改善內部流程、建構更成熟的治理體系。G總監以跨國企業為例，說明目前業界主要的三項應對策略：

1、**建立通用內部治理框架**：許多大型跨國公司正積極在內部建立統一的內部治理框架，一套共同語言與標準化規範，以便在不同司法管轄區間統一合規要求，並能持續追蹤各國法規更新與時限要求。

2、**導入自動化與 AI 技術**：企業運用人工智慧與自動化工具，依據不同地區（如 GDPR、CCPA、巴西 LGPD 等）的規範，自動調整處理流程與回應期限，提升作業效率。

3、**優化使用者請求處理（DSAR）**：透過標準化表單、自動化身分驗證與期限追蹤等數位化工具，企業能更即時地回應個人資料存取或刪除等請求。AI技術亦能更精準地在龐雜的企業資料系統中定位個人資料，確保回應的完整與正確。

現在，在歐盟GDPR架構下，要求經認證的企業必須設立有效的隱私申訴與救濟機制。當消費者向企業投訴無果時，可以進一步向「當責機構」（Accountability Agents）申訴，當責機構有權對違規組織進行懲罰，包括暫停甚至撤銷認證。因此，個人可依序向資料控制者（data controller）、監管機關（DPA）、或法院提出投訴與救濟請求。在此套層級式設計下，問題能先於企業層面獲得解決，避免訴訟程序的冗長。Gerlach表示，雖然歐盟「一站式服務」（One-Stop-Shop,OSS）制度在實務上仍有改進空間，但整體而言運作良好，且監管機關對此機制普遍持正面評價。此外，APEC（亞洲太平洋

經濟合作組織）設有一個名為CAPE（Cross-border Privacy Enforcement Arrangement）數據保護機構，促進了各參與國監管機構之間的合作執法，形成更具彈性與可執行力的跨境支援機制。

Gerlach認為儘管全球合規環境充滿挑戰，科技將在提升合規和加速救濟處理方面扮演更重要的角色，隨著 AI、資料自動化與跨境資料流通的普及，隱私治理已不再只是法律或政策的議題，而是一場結合「人、流程與科技」（people, processes, and technology）的系統性革新。企業的重點應建立一個「以人為中心」（people protection）的資料保護生態，使隱私治理從防禦轉向預防，從法規遵循升級為信任經營。

平行論壇3-A（Parallel Session 3-A）:健康資料再利用的未來：隱私、人工智慧與病患照護轉型（由OECD主導）(Re-Using Health Data: Balancing AI Health Innovation and Privacy in a Cross-Border Context (led by the OECD)：

經濟合作暨發展組織資料流通、治理與隱私處處長Clarisse Girot開場致詞

開幕致詞暨主持人：Clarisse Girot（經濟合作暨發展組織資料流通、治理與隱私處處長，Head of Division for Data Flows, Governance and Privacy, OECD）

主持人：Limor Shmerling Magazanik（經濟合作暨發展組織隱私、資料治理與數位安全政策分析師，Policy Analyst, Privacy, Data Governance and Digital Security, OECD）

主題演講：Khaled El Emam（加拿大渥太華大學醫學人工智慧加拿大研究講座教授，(Canada Research Chair, Medical AI at the University of Ottawa）

與談人：

- Nitin Dhavate（諾華醫療有限公司亞太區、中東非洲及全球健康資料隱私、數位與人工智慧主管，Head of Data Privacy, Digital & AI (DPDAI), Asia Pacific, MEA & Global Health, Novartis Healthcare Pvt. Ltd.）
- Soyoung Yoo（韓國首爾峨山醫院研究副教授，Research Associate Professor, Asan Medical Center）
- Sooyong Shin（Kakao Healthcare 首席研究官，Chief Research Officer, Kakao Healthcare）
- Gráinne Hawkes（愛爾蘭資料保護委員會副專員，Deputy Commissioner, DPC, Ireland）
- Mark J Taylor（澳洲墨爾本大學法學院教授，Professor, Melbourne Law School）
- Michael Harvey(加拿大卑詩省資訊與隱私委員辦公室委員，Commissioner, OIPC,BC Canada)

閉幕致詞：Cheongsam Yang（韓國個人資料保護委員會政策局局長，Director-General, Head of the Personal Information Policy Bureau, PIPC, Korea）

本場次由經濟合作暨發展組織資料流通、治理與隱私處Clarisse Girot處長主持，並於會中正式發布《促進跨境為公共利益目的的健康資料二

次利用（Facilitating the secondary use of health data for public interest purposes across borders Policy paper）》報告[11]。此份報告回顧自2016年OECD通過健康資料治理建議書以來的進展，強調數據共享與隱私保障是同時必須達成的公共目標，而非互相掣肘的選擇。G處長指出，隨著AI成為醫療保健領域的「系統性變革者」，現行規範的破碎化與國家間不一致已成為釋放公共利益的重大障礙。

Khaled El Emam教授進行主題演講

隨後由加拿大渥太華大學醫學人工智慧加拿大研究講座教授Khaled El Emam教授進行本次的主題演講，他在演講中提出「同意的困境」，亦即在健康數據的回顧性研究中，患者往往已遷移或過世，難以補強同意；此外，同意偏差（consent bias）會導致數據集無法代表整體人口，加劇不

[11] 報告內容請參考：https://www.oecd.org/en/publications/facilitating-the-secondary-use-of-health-data-for-public-interest-purposes-across-borders_d7b90d15-en.html

平等。E教授主張，過度依賴同意不僅限制研究效能，也可能削弱成果的社會正當性。因此，隱私增強技術（PETs）應作為二次利用的重要替代方案。

PETs包括匿名化、假名化、安全多方計算與合成數據等。E教授強調，過去幾年的技術進步使PETs在資料品質與分析實用性上已有突破，並且當數據不再屬於個人資訊時，在多數司法管轄區便可免除個別同意。這種技術路徑能減少法律障礙，提升二次利用的即時性。

然而，合法性並不等同於社會許可。E教授提出「社會許可」的概念，強調數據使用必須與社會期望一致，不得讓公眾感到驚訝。若缺乏透明度與溝通，縱使資料處理合法，仍可能導致計畫失敗。

他以兩個案例說明：

1、 **英國Care.data計畫**：因為未能清楚溝通，社會擔憂私人部門獲利，導致150萬人選擇退出，最終計畫被迫終止。

2、 **加拿大移動數據事件**：雖然數據已去識別化，且調查並未發現不當，但由於政府事後才公開，缺乏「過度溝通」，引發民眾憤怒與調查。

最後，E教授提出八項社會許可的實踐路徑，包括建立實踐規範、監管機構提前介入教育、以正面案例平衡媒體報導、提升健康素養、強調透明度、改變對商業化的負面敘事、落實代表性倫理審查，以及建立靈活迅速的審查機制。

第一場與談，與談人從左至右分別為：Limor Shmerling Magazanik、Nitin Dhavate、Soyoung Yoo、Sooyong Shin

在主題演講結束後，隨即進行第一場與談，主持人為經濟合作暨發展組織高級政策分析師Limor Shmerling Magazanik（Senior Policy Analyst, OECD），與談人則為諾華醫療有限公司亞太、中東及非洲地區資料隱私及人工智慧法規遵循主管Nitin Dhavate（DPDAI Compliance Head APMA, Novartis）、韓國首爾峨山醫院研究副教授Soyoung Yoo（Research Associate Professor, Asan Medical Center）韓國Kakao 醫療保健公司研究主管Sooyong Shin（Head of Research, Kakao Healthcare）

首先由諾華D主管分享該公司的實務經驗，其一方面透過第三方資料進行藥物安全性與依從性研究，另一方面透過內部Data42資料湖與聯邦學習機制，支援跨境臨床研究。諾華甚至利用生成式AI（如 Protocol-GPT）加

速研究設計，並實驗合成數據應用於罕見疾病。雖然GDPR提供了框架，但各國落實要求不一，跨境研究仍面臨挑戰。

峨山醫院Y教授則以具體數據展示治理效率差距：以同意為基礎建庫需長達七年、耗資二十億韓元，而假名化處理則可在兩個月內完成，成本僅百萬韓元。她的團隊建立十級風險分級制度，根據數據敏感度、環境與用途控制使用範圍，但因缺乏國家級認證，只能依賴院內工具，顯示治理碎片化問題。

Kakao醫療公司S研究主管則介紹該公司的HRS平台，與17家醫院聯盟，採聯邦學習方式推進跨院分析，將研究時間從數年縮短至不到一年。然而，他坦言涵蓋多模態數據的PETs開發是「夢魘」，同時許多醫院缺乏高效能硬體，難以支撐大型AI模型。

第二場與談，與談人從左至右分別為：Clarisse Girot、Gráinne Hawkes、Michael Harvey、Mark Taylor。

第二場與談由經濟合作暨發展組織資料流通、治理與隱私處處長Clarisse Girot主持，與談人包括加拿大卑詩省資訊與隱私委員辦公室委員Michael Harvey（Commissioner, OIPC, BC Canada）、愛爾蘭資料保護委員會執行專員Gráinne Hawkes（Deputy Commissioner, DPC, Ireland）以及墨爾本法學院教授Mark Taylor（Professor, Melbourne Law School）。

加拿大H委員的發言首先挑戰了過往常見的「隱私與數據利用對立」的假設。他指出，隱私常被誤用為拒絕分享數據的理由，然而在實務中，真正的障礙往往來自於系統互操作性的不足或資源缺乏。若將隱私過度問題化（problematizing privacy），只會削弱隱私制度的合法性，導致社會對制度失去信任。他進一步強調，治理模式應超越「以病人為本」的狹隘框架，而轉向「以人為本」，確保資料治理能涵蓋個體從出生到死亡的整個生命週期。在此脈絡下，Harvey 提倡「修復同意」而非完全超越同意，認為當同意不可行或不適用時，應以透明、包容與獨立的治理（TII governance）來補充，確保制度仍具有正當性與可接受性。

愛爾蘭H執行專員則從實務經驗出發，強調監管機構必須主動傾聽研究社群的需求。她舉例指出，愛爾蘭透過與研究界的對話，調整了規範，允許低風險的回顧性圖表審查得以免於個別同意程序，藉此兼顧研究效率與隱私保障。她也特別強調監管教育的重要性，監管機關必須協助資料保護長（DPO)以及研究人員正確解讀GDPR,避免因過度規避風險而阻礙研究進展。此外，Hawkes 指出歐洲數據保護委員會（EDPB）正在制定關於科學研究的統一指引，以緩解目前歐洲各地對於研究規範解讀的破碎化問題。她強調，隨著歐洲健康數據空間（EHDS）即將於2027年正式實施，其罰則設計將與GDPR精確對齊，這對於建立社會信任和爭取公眾支持具有關鍵意義。

墨爾本法學院T教授則聚焦於治理的基礎條件。他指出，清晰度不僅是行業運作的基石，也是社會信任的根源。監管機構應展現領導力，透過公開具體案例的調查與結果，將抽象的法律原則轉化為具體可見的實務標準，以提升透明度和預測性。進一步地，他提出「值得信任的治理」必須建構在三項要素之上，即能力（Competence）、承諾（Commitment）與文化（Culture）。此外，他闡述了公共利益測試（E-A-R）在數據治理中的價值，建議應圍繞三個核心問題展開：其一，數據的使用是否符合合理的「預期」（Expect）；其二，是否具備可被社會理解和接受的正當理由（Accept）；其三，是否尊重個人對數據的自主控制（Respect），例如異議與退出的權利。Taylor 特別警告，若制度無法獲得社會信任，最弱勢與邊緣化的群體將可能因缺乏信任而放棄與醫療系統的互動，甚至不再在臨床環境中坦誠表達自身狀況，這將嚴重削弱醫療系統的公平性與有效性。

本場次最後由韓國個人資料保護委員會政策局局長Cheongsam Yang局長進行閉幕致詞。Y局長最後作結，隱私保護應是創新的基礎，而非阻礙。韓國已建立最小化非結構化數據、釐清責任與程序的制度，並推動健康數據的安全再利用。他呼籲透過國際合作建立共通原則，讓健康數據治理能同時回應公共利益與隱私期待。

平行論壇3-B（Parallel Session 3-B）：教育科技的資料治理：如何保護兒童隱私？（由數位經濟工作小組DEWG與聯合國兒童基金會UNICEF主導）（Data Governance for EdTech:How to protect children’s Privacy? (led by the DEWG and the UNICEF)）

主持人及現場與談嘉賓，由左至右分別為Bertrand du Marais、JongYoun Rha、Zelda Gerard-Besset、Patricia Kosseim、Ivy Grace T. Villasoto、Cari Benn

主持人：Bertrand du Marais（法國國家資訊自由委員會國際事務專員，International Affairs Commissioner, CNIL, France）

主題演講：Jasmina Byrne（聯合國兒童基金會前瞻與政策處主任，Chief of Foresight and Policy, UNICEF）

與談人：

- JongYoun Rha（韓國首爾大學教授，Professor, Seoul National University）

- Zelda Gerard-Besset（法國國家資訊自由委員會法務專員，Legal Officer, CNIL, France）
- Patricia Kosseim（加拿大安大略省資訊與隱私專員辦公室專員，Commissioner, IPC, Ontario Canada）
- Ivy Grace T. Villasoto（菲律賓國家隱私委員會組長，Division Chief, NPC, Philippines）
- Cari Benn（微軟公司首席隱私長，Chief Privacy Officer, Microsoft）

本場次聚焦於「如何在快速發展的教育科技（EdTech）領域中平衡創新與兒童隱私保護」。在生成式人工智慧與自適性學習系統（adaptive learning）廣泛應用的背景下，教育科技正成為全球教育改革的關鍵驅動力。然而，技術創新同時也引發前所未有的監管挑戰。與談者從國際組織、政府、產業及學術的不同角度出發，探討在保護兒童與青少年隱私的同時，如何確保教育科技能持續推動包容性與公平的教育發展。

（一）教育科技的雙面性：創新與風險並存

講座開頭，法國國家資訊自由委員會國際事務M專員與聯合國兒童基金會前瞻與政策處B主任便共同指出，教育科技的潛力在於促進學習個人化、改善教育資源分配、提升弱勢群體的可及性。例如，AI導師系統能即時回饋學生學習狀況，減輕教師負擔。然而，這些優勢往往伴隨著風險。

B主任指出，在低與中等收入國家，教育科技的快速引入常缺乏足夠的監管與基礎設施，導致學生數據被第三方商業化使用或外流

的風險升高。這些技術系統可能不當蒐集包括學習行為、面部影像、聲音與心理特徵等高度敏感資料，形成所謂「數位監控學習環境」。

多位與談者認為，教育科技的風險不僅是技術問題，更關乎結構性不平等。若演算法訓練數據存在偏見，AI評估系統可能對特定族群或性別學生產生系統性不利結果。加拿大安大略省K專員也進一步強調，若教育科技公司未能妥善說明資料用途與安全措施，即使在合法蒐集資料的情境下，也可能違背「教育場域的信任關係」。

（二）法律框架的不足與調適

韓國首爾大學R教授指出，現行的資料保護法律多以商業資料處理為核心設計，難以回應教育場域的特殊性。以韓國為例，《個人資訊保護法》（PIPA）尚未針對AI教育應用提供明確指引，學校與科技公司在處理學生學習紀錄與影像時常陷入「合法性灰區」。

菲律賓國家隱私委員會V組長也提到，菲律賓的資料保護制度中缺乏針對兒童數據的特殊規範。教育場域中「同意」往往流於形式，學生與家長難以真正理解其資料將如何被使用。與談者一致認為，對於校園內必須蒐集與使用資料的情況，應以「履行教育任務所必要」（necessary for educational function）作為法律依據，而非要求學生或家長個別同意。

加拿大K專員則補充，加拿大在實務上要求學校進行「第三方委外盡職調查（due diligence）」以確保外包服務商遵守資料保護義務。她指出：「透明度」是現行法律體系能否有效運作的關鍵，只要教育機構能清楚揭示資料蒐集目的、處理方式與保留期限，就能增進信任與問責。

法國國家資訊自由委員會B法務專員則提及，法國正考慮在現行GDPR架構下制定教育科技附則，針對AI教學平台要求更高層級的可解釋性（explainability）與風險評估（risk assessment）標準。

（三）多方利害關係人協作與責任分配

與談者一致認為，教育科技的治理不應由單一主體承擔，而應形成「多方協作（multi-stakeholder collaboration）」的生態系。

首先，政府與監管機關是政策制定與執法的中樞，必須建立明確的規範與配套，例如資料最小化原則、兒童專屬資料保護準則等，並提供指導性文件協助學校落實規範。

其次，學校本身是教育科技的主要使用者與資料處理者。R教授指出，學校常在缺乏技術與法律知識的情況下簽署與科技供應商的合約，若未明確界定資料歸屬與使用範圍，將嚴重削弱學生權利。

產業方面，微軟公司B首席隱私長強調企業應主動將「隱私始於設計」（Privacy by Design）原則內嵌於產品研發流程中，並透過技術可視化工具（如資料流追蹤介面、透明度儀表板）讓使用者了解資料流向。

此外，家長與學生的「數位素養」（digital literacy）亦被視為最後一道防線。加拿大K 專員表示，提升學生辨識資料濫用與詐騙的能力，是防止隱私侵害的基礎工程。這需要教育部門、社群組織與平台共同合作，將隱私教育納入正式課程與教師培訓。

（四）從政策倡議到實務落地：全球案例與治理趨勢

本次也於會中分享多項具體實務案例,顯示制度落地的可能性:

1、加拿大安大略省建立了《第三方委外合約指南》(Guideline on Third-Party Procurement Contracts)與《數位隱私章程》(Digital Privacy Charter),要求學校在採購教育科技時,必須完成風險評估、設定數據保存期限並確保廠商合規。

2、韓國政府則針對「AI教科書」開發制訂技術性隱私保護指引,確保AI系統僅處理必要資料,並要求教育部設立跨部門審查小組,監督技術供應商的倫理與安全標準。

3、菲律賓NPC推動「校園資料治理模型」(School Data Governance Model),為公立與私立學校提供合約範本、資料分類原則及事件回報機制。

4、此外,UNICEF 最新報告收錄全球各國的 EdTech 實踐案例,包括以兒童參與式設計(child-centered design)建立學習平台、以及透過監管沙盒(regulatory sandbox)實驗 AI 教學工具的合規運作。

聯合國B主任強調,政策的落實關鍵不僅在於制定嚴格規範,更在於建立誘因機制,例如自願認證、隱私標章(privacy label)、及以「負責任創新」為導向的公共採購政策。她指出:「監管不能僅停留於禁止,而應促進創新生態的正向競爭。」

(五)前瞻展望:建立以兒童為中心的教育資料治理架構

與會者一致同意,未來教育科技的資料治理將朝「以兒童為中心」(child-centric)方向發展,並可分為以下4大方向:

1、**技術與倫理並重**——在AI決策過程中引入倫理審查與風險預測機制，確保技術設計符合兒童最佳利益原則。

2、**透明且可問責的資料鏈**——建立跨平台資料稽核機制，使教育部門能追蹤資料從蒐集到刪除的全流程。

3、**跨國協作與標準互認**——透過OECD、UNICEF、APPA等國際機構，推動教育科技隱私標準的互通性，以便在跨境教育平台運作時保障學生權益。

4、**持續性的數位素養培育**——讓學生、家長與教師成為積極的資料治理參與者，而非被動的資料提供者。

與談者均同意，教育科技不僅是教學工具，更是一種社會契約。唯有建立兼顧創新與人權的隱私治理體系，才能讓科技真正成為教育平等的助力，而非新的數位階層鴻溝。

肆、會議心得與建議

本屆全球隱私大會（Global Privacy Assembly, GPA）以「AI在日常生活中的運用：資料與隱私議題」為主題，深度探討人工智慧（AI）技術快速發展下，傳統資料保護框架所面臨的系統性挑戰。本次會議的核心關注點已從過往聚焦於單純的法規遵循，轉向如何在鼓勵創新、實現資料自由流動的同時，積極維護公民的隱私基本權利與人類自主性(human agency)。

本籌備處借鑒本次GPA 47的國際觀點與討論精華，謹提出以下五項心得總結與政策建議，供我國未來在個人資料保護政策與AI治理規劃上參考。

（一）擘劃新的治理生態：驅動信任治理與社會意識啟蒙

面對AI帶來的跨領域、無國界挑戰，我國應採納國際間「轉變監管思維」的共識，將資料保護機構(DPA)的角色從單純的執法者，轉變為生態系的積極促進者（facilitator）、教育者與合作夥伴。具體而言，應以「信任建構」為核心，深化公私協作夥伴關係，並推動多元化的社會認知提升計畫。

首先，觀察國際經驗建立跨部門AI治理協調平台，例如借鑒英國數位監管合作論壇（DRCF）等機制。由於AI議題已超越單一資料保護範疇，涉及競爭、安全、內容治理等層面，因此透由各部會組成常設性的協調平台，共同應對AI衍生的跨領域問題。此平台應致力於建立涵蓋政府、產業與公民社會的「多方利害關係人全球對話平台」，確保政策制定能兼顧各方利益與技術現實。

其次，建議教育與意識提升可成為未來優先推動辦理的項目。如世界銀行代表Taylor Reynolds 指出，許多新興DPA面臨社會對其

重要性認知不足的挑戰，因此我國在DPA發展的第一階段（1至3年）可優先提升社會意識。紐西蘭隱私專員Michael Webster提出的「懸崖頂上的防護欄，而非懸崖底下的救護車」理念，強調透過教育與參與來預防問題，而非僅於事後處理個案。

未來可借用此次研討會所提出之各項案例，向大眾說明隱私保護的價值，例如大規模資料外洩所造成的數千萬美元成本，藉此將隱私保護轉化為創新的驅動力（success driver），而非競爭障礙（competition barrier）。

此外，積極推動企業內部治理能力的提升，將監管壓力轉化為企業內化使用者保護的動力，例如透過提供公共財（如PETs或基礎資料集）來幫助企業建立自身的防護網。最終目標是讓AI治理的責任從政府單一監管，延伸到醫療機構、教育部門等組織的自主治理與在地化驗證。

（二）法規調適與權利保障：重塑AI時代的法律依據與集體救濟

未來建議針對AI模型訓練等新型態資料處理活動，對既有法律原則進行彈性詮釋，並優先強化資料主體的集體救濟途徑。首先，針對AI訓練數據的合法性問題，可研擬以「正當利益」（legitimate interest）為核心的適法性基礎應用指引。國際共識認為，在AI訓練這種涉及海量資料且目的動態演變的情境下，傳統以「同意」為主的適法性基礎已顯不足。愛爾蘭資料保護委員會（DPC）等機構正積極推動將「正當利益」視為更具彈性與可問責性的選項。參考此國際趨勢，或可建立一套嚴謹的「正當利益評估」框架，要求AI開

發者在主張自身利益的同時，必須證明已採取足夠強度的技術與組織措施來保障個人權利，並納入透明度與反對權等配套安全措施。

其次，建議可彈性調適「目的拘束原則」（Purpose Limitation）。此原則在AI時代面臨挑戰，可考量將其納入整體的「風險評估框架」中，根據個案情境、個人合理期待與風險緩解措施進行綜合判斷。同時，針對涉及「特種個資」（如健康資料用於消弭AI偏誤）的處理，建議積極尋求具備重大公共利益目的的法律解釋，以平衡嚴格保護與合理使用之間的兩難。

再者，建議可啟動訴訟外紛爭解決機制（ADR）的改革與強化，以確保民眾能夠獲得實質且有效的救濟。韓國公民組織Jinbonet的經驗顯示，現行爭議調解機制雖快速有效，但只要其中一方拒絕，機制便會立刻失靈，迫使受害者轉向耗時、高成本且不確定的訴訟途徑。針對個人資訊洩露等「受害者眾多但個人損害金額小」的案件，必須優先推動「真正的集體訴訟制度」，以簡化索賠流程並降低資料主體的救濟成本。

（三）推動「預防導向」稽查模式與釐清AI演進下的責任歸屬

未來，在執行相關稽查工作時，建議從傳統的「損害導向」（Harm-based）執法轉向「預防導向」（Prevention-oriented）的稽查模式，並針對AI演進帶來的「責任模糊化」挑戰，建立清晰的問責架構。首先，稽查策略應朝向「問責制強化」與「透明度提升」。

澳洲資訊專員Carly Kind提出的「監管者即顛覆者」（Regulators as Disruptors）理念，要求監管機構須主動透過執法與指導行動影響技術發展方向，建議我國未來可透過公開重大個資侵害事故

的調查報告與裁決結果之重點，將抽象之法律原則轉化為具體實務合規標準，以供外界得以遵循法律及參考；或透過執行公務機關或高風險非公務機關之事前檢查，積極輔導其採取適當安全維護措施，例如於存取假名化資料時，應建立「可信研究環境（TREs）」或「安全資料環境（SDEs）」以確保資料使用過程之安全與合規。

其次，建議監管者得因應AI應用進行相關前瞻研究，據以建立清晰「資料控制者/處理者」責任歸屬框架，特別是針對涉及多個AI代理、跨國雲端平台、第三方API之複雜產業鏈。如英國資訊委員John Edwards雖認為現有法制仍適用，但強調必須確保「人類代理權」（Human Agency）與「課責性」（Accountability），據以解決AI代理下責任模糊化及監管困境。

再者，面對DPA資源不足的挑戰，建議可學習南非多元策略。如推動修法以保留部分罰款收入以充實稽查資源；並與其他目的事業主管機關合作，建立資訊官員（DPO）的註冊制度並收取費用。在執法優先順序上，建議可集中資源應對真正具隱私高風險之場景，同時透過「監管沙盒」（Regulatory Sandbox）等機制，鼓勵企業於開發初期即與監管者互動，降低創新不確定性。

（四）隱私工程驅動：隱私增強技術（PETs）制度化與建立層級防禦機制

建議未來可積極推廣隱私增強技術（PETs）的應用，並建立標準化、可量化的風險評估框架，以技術途徑來解決AI時代下「資料最小化」與「創新需求」的矛盾。

首先，可將「假名化」（Pseudonymization）與「合成數據」（Synthetic Data）制度化。國際經驗顯示，假名化被視為平衡資料實

用性與隱私保護的關鍵技術，也是跨境傳輸的「適當保障措施」之一。後續或可研擬AI研發與應用情境下的「原則解釋指引」，提供如新加坡PDPC的「系統化五步驟流程」，協助企業理解在保障隱私前提下安全利用資料的技術範例。針對合成數據，其對於擴增小型數據集與去偏誤具有潛力，建議可建立標準化、可量化的風險評估方法論，規範其在應用時的角色與法律界定。

其次，可提前應對來自「作業系統層級」的隱私威脅。Signal基金會總裁Meredith Whittaker警示，作業系統（如iOS/Android）正轉變為整合AI代理人的主動角色，可能繞過應用程式的隱私保護措施。因此，建議未來可研議技術性要求，強制作業系統供應商提供「開發者層級的選擇退出權」（Developer-level opt-outs），以確保應用程式開發者有權拒絕作業系統層級的AI資料掃描與存取。

後續可鼓勵企業將「隱私始於設計」（Privacy by Design）原則內建於產品研發流程，例如建立「隱私評估模板」（Privacy Assessment Templates）作為開發初期的必備審查程序。針對AI支持續演進，可技術性地要求其實踐「權限最小化原則」（Least Authority Principle），嚴格限定AI代理的操作權限，防止資料外洩與權限濫用。

（五） 鏈結嵌入國際規範：透過國際合作及融合建立跨境傳輸之互通性

首先，建議未來可主動推動雙邊及多邊的資料傳輸機制對話。國際間普遍認同「資料本質上是全球流動的，但監管框架卻是在地化的」，造成監管碎片化與法遵成本巨大。因此可主動與主要貿易夥伴（如美國、歐盟、日本）進行雙邊或多邊對話，探索跨境傳輸機

制之相互承認或建立特定「資料傳輸廊道」（data transfer corridors）的可能性。同時，持續關注國際間更具彈性的「轉接頭」機制的發展，以銜接我國與各國不同的法規範差異，建立更互通性的跨境傳輸體系。

美國教授Alex Joel提醒，AI的競賽實則是民主與威權兩種價值體系的對抗，民主國家間的團結與互信是重要關鍵，故應深度參與國際多邊機制，推動全球互通性框架，作為實現「信任」機制化與規範化的路徑。如:透過OECD宣言建立共同原則、或是為中小企業量身打造簡化的行為準則或認證、或是建立如全球CBPR這樣更具互通性的體系，將「信任」機制化。

再者，建議可強化國際合作以應對跨國執法困境。義大利對Clearview AI裁罰2,000萬歐元後，因缺乏與美國的雙邊強制執行協議而難以落實。故建議未來可致力於透過全球隱私保護組織（GPA）或APEC的CAPE等機制，採取集體行動，以共同制衡違反多國法律的跨國企業，避免讓國內資料主體的權利因跨境而失靈。

（六）結論

本次全球隱私大會的核心主題—人工智慧與隱私保護—明確指出，全球資料保護正進入一個以「信任建構」為核心的新治理時代。傳統上以靜態法規遵循為主的單一監管模式，已無法應對AI時代下資料處理的複雜性與自主性。透過以上具體策略與建議，期望我國個資保護與人工智慧的潛力得以在安全、負責的框架下實現，確保創新與隱私並非對立，而是相互促進、相互強化的關係，如歐盟委員Michael McGrath所言：「沒有資料保護，就沒有值得信賴的AI。」

籌備處同仁參與GPA 47大會合影