



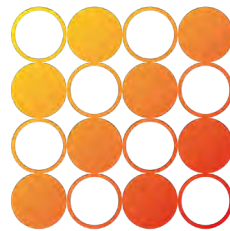
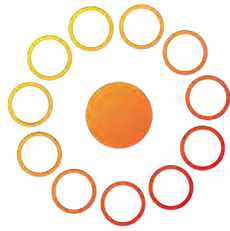
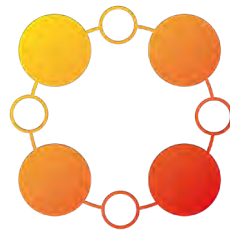
JERSEY 2024

HOST NATION'S REPORT

Paul Vane

JANUARY 2025





CONTENTS

Conference by Number	4
Conference Feedback	5
Introduction and Executive Summary	6
Locations Used	7
Conference Theme: The Power Of 'I'	8
Programme	12
Day 1: Monday 28th October 2024	18
Day 2: Tuesday 29th October 2024	19
Day 3: Wednesday 30th October 2024	38
Gala Dinner and Awards Ceremony	49
Side Events	56
Common Themes Arising Across all Pillars	57
Action Points Arising	60
Lessons Learned from Organising a Major International Conference	63
Social Media Engagement and Performance	65
Local Economic Impact	67
Delegate Feedback	68

Appendices

Appendix 1: Full Speaker List	70
Appendix 2: Sponsors	73
Appendix 3: Financials	73
Appendix 4: With thanks to...	74



CONFERENCE BY NUMBERS

70

COUNTRIES
REPRESENTED



500

DELEGATES

80

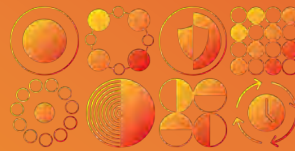
SPEAKERS
OVER 3 DAYS

122



DATA PROTECTION
AUTHORITY DELEGATES

8



PILLARS OF THE
'POWER OF I' THEME

27

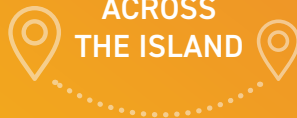
SESSIONS
OVER 3 DAYS

14

SIDE EVENTS
ACROSS THE
FULL WEEK

SEVEN

VENUES USED
ACROSS
THE ISLAND



17

SPONSORS

282

EUROPEAN DELEGATES

OF THE DELEGATES THAT COMPLETED THE POST EVENT SURVEY:

85%

said the conference theme
addressed current trends
and challenges in privacy
and data protection very or
extremely effectively.

95%

rated the quality of
the speakers and
panel members
as very good or
extremely good.

83%

said the conference succeeded very
or extremely well in fostering a
deeper understanding of the cultural
and behavioural changes needed
around the use of personal data.

CONFERENCE FEEDBACK COMMENTS

'JOIC did a fantastic job as host'

'The youth panel was particularly powerful and thought provoking'

'Loved the panel with indigenous people talking to Data Protection. So excellent and important'

'I think the biggest theme that became apparent was the need for more collaboration'

'The Privacy Debate: What the Next Generation Think gave us the opportunity to rethink our strategy. The live and frank voices of the next generations urged us to review whether our current initiatives reflect practical needs or demands of citizens'

'Loved the new perspectives and focus on topics outside of what we hear all the time. Fantastic conference'

'Inviting 'real' young people as panellists was a great move. It was really refreshing and valuable to put the spotlight back on the people we aim to protect, instead of just giving the stage to authorities'

'My hope is that indigenous will now get some much-needed attention'

'The ideas on data protection authorities being fit for the 21st century is also important for DPAs to change to be better regulators in the digital/AI world'

'Involving young people's voices in the children's privacy panel in the Open Session was an excellent idea'



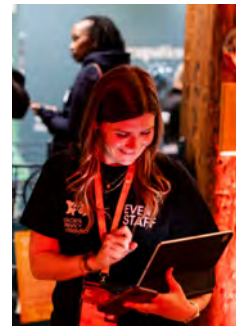
EXECUTIVE SUMMARY

During the week commencing 28th October 2024, Jersey played host to the Global Privacy Assembly Annual Conference. Attracting over 500 delegates from more than 70 different countries, it was an honour and a privilege for the Jersey Data Protection Authority to welcome attendees to its shores and showcase Jersey and all it has to offer.

In hosting the GPA Annual Meeting 2024 the organisers wanted guests to enjoy the spirit and hospitality of their island nation, a place where collaboration and innovation thrives. A wealth of local leaders, industry bodies, event suppliers and experts came together to make the Jersey conference unforgettable.

This report details the full programme of events with a summary of content of each of the sessions during the open part of the conference week. The report highlights the outcomes and action points arising from the conference sessions and creates a roadmap for the future. It is also designed to provide a blueprint framework for future conference hosts, detailing budgetary considerations, lessons learned during the months of preparation leading up to the conference week, and the positive impact on the local Island economy.

Finally, the report will pay tribute to the speakers, sponsors, advisers, creative designers and events team that worked tirelessly over two years to bring a conference concept to life. We hope the report provides a comprehensive overview of the important privacy discussions that took place across the event, and illustrates the value created by the event in terms of advances in privacy policy, enhancement of individual privacy rights and the economic benefit to the Island of Jersey.





LOCATIONS USED

Steeped in history and known for its beautiful beaches and coastline, Jersey is a tourist destination with a rich and diverse past. A British Crown Dependency 100 miles from the south coast of England and just 14 miles from France, Jersey is the sunniest spot in the British Isles with a delightfully continental twist. It is home to an international finance centre and has some of the fastest broadband speeds in the world.

Jersey is a self-governing British Crown Dependency. It is the largest of the Channel Islands, independent of the United Kingdom and has its own Government, legal and monetary systems, including the Jersey Pound. Within the British Common Travel Area, Jersey is home to 108,000 diverse residents who speak an array of languages including English, Portuguese, Romanian, Polish, French and Nigerian. Our official languages are English, French and Jèrriais.

Given the geographical size of the Island, and the uniqueness of the location, which was alien to many, it was decided that Jersey's conference would be a multi-venue event taking in a number of different locations and venues across the whole Island. This would allow visiting delegates to experience as much as Jersey as possible, whilst still allowing for a full programme of topics.

The venues utilised were:

- Jersey Maritime Museum, St Helier (Welcome Reception, day 1)
- Royal Jersey Showground, Trinity (Open Session and Gala Dinner, days 2 & 3)
- The Radisson Blu Waterfront Hotel, St Helier (Side events and Closed Session, days 4 & 5)
- La Mare Wine Estate, St Mary (Side event, day 3)
- Pomme D'Or Hotel, St Helier
- Grand Hotel, St Helier



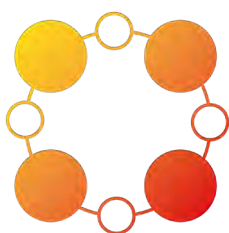
CONFERENCE THEME



Individuals



Innovation



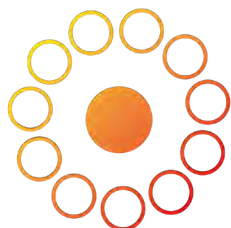
Integrity



Information



Independence



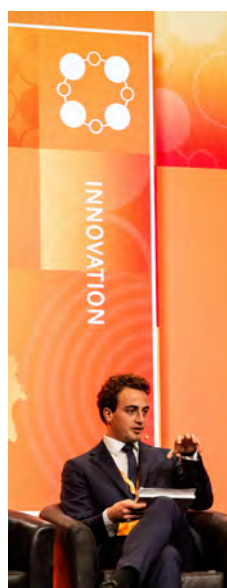
International



Intercultural



Indigenous



THE POWER OF 'I'

'The Power of I' was the overarching theme for the 2024 Annual Conference. It highlights the significance of the eight themes, which are intrinsically linked to encompass the harms, values, and enrichment of our human lives. The Conference sought to establish and explore how we can respect and balance the power of information with the need for citizens across the world to have power, control, and dignity over their personal information. The discussions challenged and questioned who controls this power, for what purpose, and for whom. They also examined the effectiveness of current regulatory models, questioning whether they are still fit for purpose in a rapidly changing world. The overarching aim of the conference was to create a roadmap for the future, both short-term and long-term, to improve individuals' ability to self-manage their data, achieve greater equity in data sharing, and foster better behaviours and culture around the use of personal data.

1. Individuals

At the heart of privacy is the individual, and understanding this is critical when designing effective protection mechanisms. Privacy is not just a legal concept or a technical challenge; it's a deeply personal concern. Each individual possesses a unique set of preferences, boundaries, and sensitivities, making a one-size-fits-all approach inadequate.

By recognising the uniqueness of individuals, we can begin to understand the diverse ways people interact with technology and share information. Tailoring privacy measures to individual needs ensures that autonomy and personal choices are respected. This perspective helps give users the power to define their own level of privacy.

Putting the individual first acknowledges the ethical dimension of privacy. Respecting personal autonomy becomes a foundational principle, fostering a culture of trust between users and technology providers. It reinforces the idea that privacy isn't an inconvenience to be circumvented but a fundamental right that should be upheld.

Essentially, individuals are not passive recipients of privacy; they are active participants, shaping the contours of their digital boundaries. Recognising this centrality empowers people in the digital age, ensuring that privacy measures align with the unique expectations and values of each person.

2. Innovation

In a rapidly evolving digital landscape, innovation is both pivotal to safeguarding the future of privacy and works in harmony with privacy regulation, with regulation being an enabler for innovation. As technology advances, so do the methods of data collection and analysis, posing unprecedented challenges to personal information security. Innovative solutions become the bulwark against emerging threats, ensuring that individuals can navigate the digital realm with confidence.

Innovations in encryption, decentralised technologies, and artificial intelligence can be crucial for developing robust privacy measures. They can empower users with greater control over their data, mitigating the risks associated with new and emerging technologies.



In addition, innovative advancements in artificial intelligence allow for the creation of adaptive privacy tools. AI algorithms can proactively identify and respond to evolving privacy risks, enhancing the resilience of protective measures. As privacy concerns continue to morph in complexity, a commitment to innovation becomes synonymous with preserving personal freedoms.

Innovation is therefore crucial in helping protect privacy for the future. Without continuous advancements, the battle against invasive technologies and malicious actors becomes increasingly challenging. By embracing innovation, we not only address current threats but also develop a dynamic defence system that can withstand the ever-changing landscape of privacy challenges.



3. Information

Information sits at the very hub of personal data protection. Information, encompassing details about individuals, their activities, and preferences, is the currency of the digital age. Safeguarding this is essential for preserving the integrity of personal privacy and choices.

Privacy hinges on controlling the flow and access to information. In the digital era, vast amounts of data are generated daily, from online interactions to biometric details. The power to dictate who collects, processes, and shares this information is fundamental to maintaining personal agency. Without robust privacy safeguards, information becomes vulnerable to misuse, potentially infringing on individual freedoms.

Furthermore, information shapes how individuals are perceived and treated, thus the importance of protecting personal information cannot be underestimated. Good data protection practices help to create a shield against unwarranted intrusion and manipulation, enabling individuals to exercise a degree of control over their personal information in alignment with their values.

Information is the cornerstone of privacy, underlining its importance in the protection of personal freedoms. Acknowledging the significance of information in the privacy discourse is key to navigating the complex landscape of the interconnected world while upholding individual rights and dignity.

4. Integrity

Integrity forms the backbone of privacy, ensuring that personal information is handled with honesty, consistency, and reliability. When privacy measures lack integrity, trust between individuals and organisations tasked with managing their data erodes. Unauthorised access, data loss, or deceitful practices, jeopardise the sanctity of personal information.

Maintaining the integrity of privacy measures is crucial for instilling trust and confidence in users. When individuals entrust their information to platforms or services, they expect these organisations to uphold the agreed-upon principles and protect their information with the highest ethical standards. A breach in integrity not only violates this trust but also exposes individuals to risks ranging from identity theft to irreversible harms.

Integrity also plays a pivotal role in ensuring the accuracy of information. Inaccurate data, whether intentional or unintentional, can lead to flawed decision-making processes, perpetuating misinformation, and potentially harming individuals. Upholding the integrity of privacy practices means committing to accurate data representation, contributing to a more transparent and reliable digital landscape.

Integrity is a critical pillar of effective privacy protection. It builds a foundation of trust, reliability, and transparency, essential for navigating the complexities of a data-driven world while safeguarding the fundamental right of individuals to control and secure their personal information.

5. Independence

Independence is key to effective privacy regulation, ensuring that oversight and enforcement are impartial and free from undue influence, particularly from Government. Data Protection Authorities must operate independently to maintain a balance between the interests of individuals, businesses, and society at large. This autonomy allows regulators to act in the public interest without succumbing to external pressures that might compromise the privacy rights of individuals.

An independent regulatory framework is essential for adapting to the dynamic nature of technology and emerging privacy challenges. It enables regulators to swiftly respond to evolving threats, enact necessary reforms, and enforce compliance with privacy standards. Without independence, regulatory bodies may be hindered in their ability to keep pace with the rapid advancements in the digital landscape.

In addition, independence fosters credibility and trust in the regulatory process. Individuals, businesses, and other stakeholders are more likely to adhere to privacy regulations when they have confidence in the impartiality and integrity of the overseeing Data Protection Authority. This trust is essential for cultivating a culture of respect for privacy rights and encouraging widespread compliance.

Independence in privacy regulation is fundamental for creating a robust and adaptive framework that safeguards individuals' privacy. It ensures that privacy protections remain resilient, transparent, and capable of addressing the ever-changing dynamics of the digital era.

6. International

The 'International' in our theme focused on the global nature of privacy, recognising the diversity of countries and territories and acknowledging that privacy crosses borders.

Cooperation among data protection authorities is imperative for effective privacy regulation in our globally interconnected world. The digital landscape knows no borders, and data flows seamlessly across jurisdictions, making collaboration essential to tackle cross-border privacy challenges.

By working together, data protection authorities can share insights, best practices, and intelligence on emerging privacy threats. This collaboration enables a more comprehensive understanding of evolving risks, ensuring that regulatory responses are both timely and informed. It allows authorities to harmonise approaches, promoting consistent standards that protect individuals' privacy rights, regardless of their location.

This unified approach strengthens the deterrent effect of privacy regulations, discouraging unethical practices on a global scale. Sharing resources and expertise enhances the collective ability to address complex privacy issues, providing a more robust defence against threats to individuals' personal information.

The creation of a cohesive and effective global privacy framework that recognises our diverse make up cannot be underestimated. It acknowledges the interconnected nature of data and ensures that privacy protections extend beyond borders, reinforcing the fundamental right to privacy in an increasingly interdependent world.

7. Intercultural

Intercultural understanding plays a pivotal role in shaping privacy regulations that resonate with diverse global communities. Privacy norms and expectations vary significantly across cultures, influenced by distinct values, societal norms, and historical contexts. To craft effective regulations, it is crucial for policymakers and regulators to appreciate these cultural nuances.

Respecting intercultural differences in privacy frameworks ensures that regulations are not one-size-fits-all but instead accommodate the diverse needs and expectations of individuals worldwide. Cultural sensitivity in privacy regulation acknowledges that what may be acceptable or intrusive in one culture may differ in another, preventing the imposition of rigid standards that could hinder global cooperation.

It also promotes inclusivity in the regulatory process, allowing for diverse voices to be heard, ensuring that the perspectives of individuals from various cultural backgrounds contribute to the formation of comprehensive and equitable privacy protections. This inclusivity is essential for building trust in the regulatory framework, as it reflects a commitment to respecting the autonomy and values of all individuals.

The development of privacy regulations that are not only effective but also respectful of the rich tapestry of global cultures is essential if we are to foster a more inclusive, adaptable, and universally accepted approach to privacy protection in our interconnected world.

8. Indigenous

Indigenous cultures often have distinct approaches to information sharing, communal decision-making, and the significance of personal data. Crafting effective privacy regulations requires an appreciation for these cultural intricacies.

Respecting indigenous cultures in privacy regulation acknowledges historical injustices, including colonial practices that often resulted in the exploitation of indigenous knowledge and resources. By understanding and incorporating indigenous perspectives, regulations can be designed to rectify past wrongs, ensuring that the privacy rights of indigenous individuals are safeguarded.

Furthermore, indigenous communities often have communal notions of ownership and governance, challenging traditional Western concepts of individual privacy, some more innovative than we perhaps give credit for. Recognising and respecting these communal values in regulation is essential to avoid imposing frameworks that may not align with the cultural norms of indigenous peoples.

Incorporating indigenous voices in the regulatory process ensures a more inclusive and equitable approach to privacy. It reflects a commitment to justice, acknowledging the importance of cultural diversity in shaping regulations that protect the rights and autonomy of all individuals, including those within indigenous communities.



PROGRAMME

MONDAY 28TH OCTOBER 2024

TIME	SESSION	SPEAKERS
12.00 – 16.00	Afternoon side events and meetings	Various
18.30 – 21.00	Welcome Reception and drinks Jersey Maritime Museum	Paul Vane Jacob Kohnstamm Elizabeth Denham John Henry Falle

TUESDAY 29TH OCTOBER 2024

TIME	SESSION	SPEAKERS
08.00 – 09.00 Main Hall	Registration, welcome pack and refreshments	None
09.00 – 09.05 Main Hall	Opening remarks and welcome from Information Commissioner	Paul Vane, Jersey Information Commissioner
09.05 – 09.10 Main Hall	Opening address and welcome from the Government of Jersey Minister for Sustainable Economic Development, Deputy Kirsten Morel	Deputy Kirsten Morel, Government of Jersey
09.10 – 09.30 Main Hall	Keynote Presentation: "Exponential Identity - Anticipating Intelligence Augmentation"	Nik Badminton, Futurist
09.30 – 10.15 Main Hall	Fireside Chat: The impact of AI	Moderator: Elizabeth Denham Panellists: <ul style="list-style-type: none"> • Julie Brill, CPO Microsoft • Teki Akuetteh, Africa Digital Rights Hub • Boniface De Champris, Computer & Communications Industry Association, Brussels • Miriam Wimmer, Director, National Data Protection Authority Of Brazil

TUESDAY 29TH OCTOBER 2024 (CONTINUED)

TIME	SESSION	SPEAKERS
10.15 – 10.45 West Wing	Refreshment & Networking break	
10.45 – 11.05 Main Hall	Keynote Presentation: "Who Cares About One Person? How Elevating the Individual Elevates all Humanity"	Douglas Kruger, International Inspirational Speaker
11.05 – 11.50 Main Hall	Panel Discussion (With A Difference)	Moderator: Paul Breitbarth, Jersey Data Protection Authority Panellists: 3x Local Youth Representatives
12.00 – 12.45 Room 1	Parallel Session: Data Protection And Mental Health	Moderator: Advocate Davida Blackmore, Principal (Advocate DVB) and Chairman Of The Mental Health Review Tribunal (Jersey). Panellists: <ul style="list-style-type: none"> • Alvaro Badoya, Commissioner, Federal Trade Commission • Wojciech Wiewiorowski, European Data Protection Supervisor • Dan Holloway, CEO & Founder, Rogue Interrobang
12.00 – 12.45 Room 2	Parallel Session: "Defining Privacy Harms In A Modern World"	Moderator: Bojana Bellamy, President, Centre for Information Policy Leadership Panellists: <ul style="list-style-type: none"> • Anu Talus, Chair, European Data Protection Board • Emily Keaney, Deputy Commissioner, Ukico • Andy Phippen, Professor, Bournemouth University (C/O Meta) • Jade Nester, Director, Data Public Policy, Europe, TikTok
12.00 – 12.20 Main Hall	Keynote Presentation: "How Technology Will Impact The Regulator: What Does Our Future As Digital Regulators Look Like?"	Marie-Laure Denis, Chair Of The Commission Nationale Informatique & Libertés (CNIL)
12.20 – 13.00 Main Hall	Panel Discussion: "Regulatory Cousins"	Moderator: Trevor Hughes, CEO, IAPP Panellists: <ul style="list-style-type: none"> • Christopher Hodges OBE, Chair, Regulatory Horizons Council; Emeritus Professor Of Justice Systems, Oxford University • Noriswadi Ismail, Senior Director For Data Privacy, GSMA • Thibault Schrepel, Associate Professor Of Law At The Vrije Universiteit Amsterdam, Faculty Affiliate At Stanford University • Emma Redmond, Open AI
13.00 – 14.00 West Wing	Buffet Lunch	

TUESDAY 29TH OCTOBER 2024 (CONTINUED)

TIME	SESSION	SPEAKERS
14.00 – 14.45 Main Hall	Panel Discussion: "The Advantages And Challenges Of Data Transfer Tools"	Moderator: Joe Jones, Research Director, IAPP Panellists: <ul style="list-style-type: none"> • Clarisse Girot, Acting Head, Division on Data Flows, Governance and Privacy, OECD • Estelle Masse, Policy Officer, International Affairs and Data Flows, Directorate-General for Justice, European Commission • Commissioner Yuji Asai, Personal Information Protection Commission, Japan • Haksoo Ko, PIPC Korea
14.45 – 15.30 Main Hall	Panel Discussion: "International Transfers In The Context Of Financial Services - What Is The Direction Of Travel? What Does The Future Look Like For Data Transfer Mechanisms?"	Moderator: Vivienne Artz, Senior Data Strategy & Privacy Policy Advisor to the Centre for Information Policy Leadership. Panellists: <ul style="list-style-type: none"> • Lori Baker, Director of Data Protection, Dubai International Finance Centre Authority • Jill Britton, Director General, Jersey Financial Services Commission • Katherine Race Brin, Chief Data Privacy Officer, The World Bank
15.30 – 16.00 West Wing	Refreshment & Networking Break	
16.00 – 16.20 Main Hall	Keynote Presentation: "The Role Of Data Privacy In Humanitarian Crises"	Massimo Marelli, Head of Data Protection Office, International Committee of the Red Cross (ICRC)
16.20 – 17.15 Main Hall	Panel Discussion: "How Do Indigenous Communities Develop Their Own Data Protection Frameworks?"	Moderator: Malcolm Crompton, IIS Partners Panellists: <ul style="list-style-type: none"> • Immaculate Kassait, MBS, Data Commissioner/1st Vicechair, Network of African Data Protection Authorities (NADPA) • Josefina Roman Vergara, Commissioner, Mexico INAI • Shana Morgan, Global Head of Privacy & AI Compliance, L3Harris Technologies
17.15 – 17.30	Reflections on Day 2	Master of Ceremonies, Richard Purcell, CEO, Corporate Privacy Group

WEDNESDAY 30TH OCTOBER 2024

TIME	SESSION	SPEAKERS
08.00 – 08.30 West Wing	Coffee and Refreshments	
08.30 – 08.40 Main Hall	Re-Cap Of Day 2	Master of Ceremonies, Richard Purcell, CEO, Corporate Privacy Group
08.40 – 09.00 Main Hall	Keynote Presentation: "Reducing Inequalities In Privacy Rights: Exploring The Different Privacy Dimensions Of Diversity"	Kate Wright, Director, Arbre Consulting, Co-Founder Of The Diversity Network Jersey
09.00 – 09.45 Main Hall	Panel Discussion: Education From The Ground Up: The Societal Impact Of Privacy Education	Moderator: Patricia Kosseim, Privacy Commissioner For Ontario, Canada Panellists: <ul style="list-style-type: none"> • Matthew Johnson, Director of Education, Media Smarts • Baroness Beeban Kidron OBE, Member of the House of Lords, Founder & Chair 5Rights Foundation • Bertrand du Marais, Commissioner, CNIL • Leanda Barrington-Leach, Executive Director, 5Rights Foundation • Joyce Lai, Assistant Privacy Commissioner for Personal Data (Corporate Communications and Compliance), PCPD
09.45 – 10.30 Main Hall	Panel Discussion: Accessible Privacy: Protecting The Disabled, Vulnerable And Socially Marginalised In A Digitised World	Moderator: Alex White, Commissioner, Bermuda Panellists: <ul style="list-style-type: none"> • John Edwards, Information Commissioner, UK ICO • Philippe Dufresne, Commissioner, Office of the Privacy Commissioner, Canada • Beatriz Anchorena, AAIP Argentina Director • Carly Kind, Privacy Commissioner, Office of the Australian Information Commissioner
15.30 – 16.00 West Wing	Refreshment & Networking Break	
11.00 – 11.45 Main Hall	Panel Discussion: Creating Trust Through Data Trusts	Moderator: Rachel Harker, Digital Jersey Panellists: <ul style="list-style-type: none"> • Dame Wendy Hall, Regius Professor of Computer Science, University of Southampton • Jack Hardinges, Independent Consultant, Foresight • Carolyn Lang, Pinsent Masons

WEDNESDAY 30TH OCTOBER 2024 (CONTINUED)

TIME	SESSION	SPEAKERS
11.45 – 12.30 Main Hall	Panel Discussion: Trust And Safety For Automobile Innovation	Moderator: Dan Caprio, Co-Founder and Chairman, The Providence Group Panellists: <ul style="list-style-type: none"> Maarten Botterman, Director, GNKS Consult BV Jonathan Cave, Academic Economist and Associate at GNKS Andreea Lisievici Nevin, Privacy Digital and AI Consultant, Trainer and Mentor, Privacy Craft
12.30 – 13.00 Main Hall	Catwalk Debate: Data Minimisation: A True Guidance Point, Or A Relic?	Moderator: Jules Polonetsky, Chief Executive Officer, Future of Privacy Forum Red Corner: Philippe Dufresne, Privacy Commissioner Of Canada Blue Corner: Sheila Colclasure, Global Chief Data Integrity and Public Policy Officer
12.30 – 13.00 Room 1	Parallel Session: Data Sharing Between Government And Third Sector	Moderator: Gerlach, Director for Privacy & Data Policy, Centre for Information Policy Leadership Panellists: <ul style="list-style-type: none"> Mark Coxshall, Chief Executive Officer, EyeCan Massimo Marelli, Head of Data Protection Office, International Committee of the Red Cross (ICRC) Yukiko Lorenzo, Senior Vice President, Assistant General Counsel, Privacy and Data Protection, Mastercard
12.30 – 13.00 Room 2	Parallel Session: The Benefits & Drawbacks Of Regtech - Are They Just Privacy Washing?	Moderator: Dr. Gabriela Zanfir-Fortuna, Vice President for Global Privacy, Future of Privacy Forum Panellists: <ul style="list-style-type: none"> Steve Tan, Partner, Rajah & Tann Singapore Jane Horvath, Partner, Gibson, Dunn & Crutcher Justin S. Antonipillai, Founder and CEO, Stewardshipped.ai & Senior Advisor - Gretel
13.00 – 13.20 Main Hall	Fireside Chat: Coping With The Extreme	Martine Wright Mbe (Interviewed By Jess Dunson, ITV Jersey)
13.20 – 13.25 Main Hall	Closing Remarks From The Assistant Minister For Sustainable Economic Development, Government Of Jersey	Deputy Moz Scott
13.25 – 13.30 Main Hall	Closing Remarks From GPA24 Host And Information Commissioner, Paul Vane	Paul Vane, Information Commissioner, Jersey Office Of The Information Commissioner

WEDNESDAY 30TH OCTOBER 2024 (CONTINUED)

TIME	SESSION	SPEAKERS
15.30 – 16.00 West Wing	Takeaway Lunch Provided	
13.35	Coaches To St Helier	

SIDE EVENTS

13.30 – 17.00	Afternoon Side Events And Meetings	Various
---------------	------------------------------------	---------

GALA DINNER

17.30 – 18.00	Transport From St Helier To Royal Jersey Showground	
17.30 – 18.00	Welcome drinks, Royal Jersey Showground	
19.00 – 21.30	Dinner Service	
21.15 – 21.30	Address From Commissioner Didier Reynders, European Commission	Commissioner Didier Reynders, European Commission
21.30 – 22.00	Global Privacy Assembly Awards Ceremony	Paul Vane, Information Commissioner, Jersey Office Of The Information Commissioner Josefina Roman Vergara, Commissioner, Mexico Inai
22.00 - 23.00	Evening entertainment from local party band, Inside Job	

**The Closed Session agenda took place on Thursday 31st October and Friday 1st November are not detailed on this programme.

DAY 1: MONDAY 28TH OCTOBER 2024

A NUMBER OF SIDE EVENTS WERE HELD DURING THE COURSE OF DAY 1:



Meeting of the Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP) – Radisson Blu Waterfront Hotel



Meeting of the GPA International Enforcement Working Group - Radisson Blu Waterfront Hotel



Side Session on International Data Protection Certification: Convergence and Interoperability, sponsored by Mandat International – Pomme d'Or Hotel



Side Session Roundtable: Smart Data Privacy Implementation, sponsored by GSMA – Radisson Blu Waterfront Hotel

The formal Welcome Reception took place at the Jersey Maritime Museum early on Monday evening. Hosted by Jersey Information Commissioner, Paul Vane, all delegates were invited to attend the reception.



DAY 2: TUESDAY 29TH OCTOBER 2024

OPENING REMARKS

Deputy Kirsten Morel, Minister for Sustainable Economic Development

Deputy Morel welcomed attendees from around the world to the 46th Global Privacy Assembly, and expressed gratitude to the Information Commissioner for the introduction.

He talked about how Jersey's international outlook shapes its identity and economy; as a crown dependency, it manages its own legislation. He touched on the importance of economic success and attracting customers globally, its historical industries include shipbuilding, textiles, and financial services.

Deputy Morel placed an emphasis on stability, quality, and adherence to global best practices in data protection, recognising technological change as both an opportunity and a challenge and the need for collective navigation. He focused on the importance of fostering innovation and entrepreneurship to leverage Jersey's data protection regime, giving the example of an operational data trust initiative launched by Digital Jersey with the Jersey Office of the Information Commissioner.

He called for collaboration among governments, regulators, and businesses to prioritise data privacy, stating that every individual has a role in data security, and acting responsibility in the use of modern technology.

Deputy Morel gave a personal reflection on privacy as a fundamental human right, influenced by experiences during the Cold War. He voiced concerns about the erosion of privacy in today's digital age and the importance of placing a value on privacy, especially for younger generations, highlighting the significance of the conference in raising global standards for data protection and privacy.

The Minister reaffirmed how Jersey seeks proactive collaboration with other jurisdictions and technology providers for effective regulation. He recognised we are at a critical moment regarding the safety of widely used technologies, especially concerning children and young people, and ensured a commitment to the safety and privacy of citizens in the context of technological advancements. Deputy Morel applauded the Jersey Office of the Information Commissioner for their educational work, commenting that helping people understand how to be safe is as important if not more important than a purely regulatory approach.

He emphasised that small jurisdictions like Jersey can contribute to developing effective regulatory systems, especially in the context of AI growth, with collaboration with tech platforms and developers being essential for enhancing online safety and privacy while enabling product development. Deputy Morel called for collective effort to ensure safety for Jersey, Europe, and the global community.



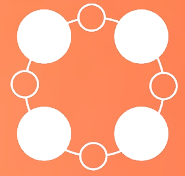
Deputy Morel concluded with an acknowledgment of the work of the outgoing Chair of the Jersey Data Protection Authority, Jacob Kohnstamm, for his significant contributions over the past four years, recognising his role in shaping data protection attitudes in Jersey and Europe. He expressed gratitude and honour for working with Jacob, while looking forward to collaborating with incoming Chair, Elizabeth Denham.

Key Points:

- Emphasis on stability, quality, and adherence to global best practices in data protection to navigate the opportunities and challenges faced by emerging technologies;
- Focus on the importance of fostering innovation and entrepreneurship to leverage Jersey's data protection regime;
- Call for collaboration among governments, regulators, and businesses to prioritise data privacy;
- Important to place a value on privacy, especially for younger generations;
- Small jurisdictions like Jersey can contribute to developing effective regulatory systems, especially in the context of AI growth.



SESSION 1 – INNOVATION



KEYNOTE SPEECH

Nik Badminton, Futurist

Exponential Identity - Anticipating intelligence augmentation

Nik started his speech talking about the constant hype around technology over decades and corrected the mainstream narrative but saying that we are not moving faster than we've ever moved before. It's just noisier than it was before.

Nik talked about how the foundation part of what we do is a focus on hope, which is about setting goals, having pathways forward and giving agency to all. He said that futurists scan for signals, looking for things that orchestrate change. They look at trends, scenarios, the dynamics of change and storytelling – this is important because once we can create a story, we can feel what it's like. Futurist work is about igniting imagination, building anticipation for what comes next, and deepening an empathy of who in the world we serve.

He referred to Apple's former CEO and Founder, Steve Jobs, who ignited the imagination in 1984 with a dystopian view of the future, and created Apple, based on the creation of personal freedoms.

Nik emphasised how the real power in the world is to change our mindset from 'what is' to 'what if'. He went to talk about how identity links all of the 8 Pillars of the Power of 'I' and how our identities have been under scrutiny...Who are we online? Emojis are a categorisation of our emotions. Our emotions create our identity. Our identity goes through cycles. He moved onto Generative AI, claiming that everything is over hyped and how all the worry we had hasn't come to pass. He advised that the people who are working against us and who we need to be concerned about are those who are collecting data to train the algorithms that will be used in the next cycle of elections. He reminded us of the 70 elections taking place in the next 2 years and warned that it's training data for the next wave of misinformation.

Nik talked about how the world is becoming more autonomous through "Agentic AI", and how we have become more 'digifrenic' living in a 'hyper-reality', gamified existence as we develop multiple personalities online. But also, how we can level our

businesses by freeing up some of the menial data processing tasks to focus more on strategic planning. He predicted that data will grow faster, and by 2050, it will be 1000 times faster than it is today.

Nik questioned what the guardrails are we give individuals to cope with these changes. He asked if we give that power to the individuals to manage and what flexibility we give humans to live their lives. He quoted Amara's law: In the short term we tend to overestimate the impact of technology. But in the long term, we always underestimate its impact, giving the example of Kodak with the digital camera, and Blockbuster with the internet for example.

To conclude, Nik advised we do 4 things: 1) Scan for signals 2) Look for trends 3) Ask what if? 4) Start telling stories. He said that futures work is about questioning everything. Question our own history and perspective. He recommended looking for pockets of the future in the present and to be wildly creative and collaborate. And finally to shift our mindset from 'What is?' To 'What if'

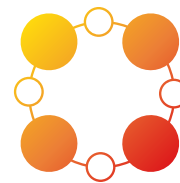
Key Outcomes:

- Technology is not moving faster, but the noise is getting louder and data is getting bigger.
- If we want to change the world, we need to change our mindset from 'what is' to 'what if'.
- Our emotions create our identity. Be careful with those who try to influence it.

Action Points:

- Don't underestimate the long-term impact of technology.
- Scan for signals
- Look for trends
- Ask 'What if?'
- Start telling stories.

SESSION 1 – INNOVATION



FIRESIDE CHAT

This session looked at the impact of AI and addressed questions such as, “How do we change our mindset to deal with advanced analytics? What part do ethics play in adjusting that mindset? How will our fundamental human rights be affected? Does AI compliment Data Protection or is it in conflict? Do we have a vision of how to be regulators of analytics in an emerging world?”

MODERATOR:

Elizabeth Denham CBE

PANELLISTS:

Cari Benn, Associate General Council Microsoft

Teki Akuetteh, Africa Digital Rights Hub

Boniface De Champris, Computer & Communications Industry Association, Brussels

Miriam Wimmer, Director, National Data Protection Authority of Brazil

Panel Chair, Elizabeth Denham started by describing how much of our environment is in a state of flux, with a tsunami of new laws creating cross-regulatory tensions. She talked about how DPAs are expected to do more, but with less resource.

Ms Denham asked the panel to discuss the unique challenges being faced in the AI world. Ms Wimmer stated that Brazilian law has a strong focus on human rights, but there are challenges building a culture of data protection in a country of 212 million. She said there were complex intersections between the new AI regulation and existing legislation, and it was challenging to deal with global players who are not as eager to participate. The country is still on a learning curve, but the DPA is starting to enforce more.

Ms Denham asked Ms Akuetteh what she was seeing in a jurisdiction where data protection law was still new, and where compliance is constrained due to a lack of resources. Ms Akuetteh said the situation was similar to Brazil, but now there were 36 African countries with DP laws, 20 of which have an authority. She said DPAs needed to be agile as the adoption of new technology was seized upon quickly, and it was difficult to get adequate resource to help them address the issues and keep up. Ms Akuetteh said this was problematic when DPAs are seen as central to the AI ecosystem and needed to be proactive.

Ms Benn was asked about the challenges and opportunities that are unique to Microsoft, and how they hyper-scale its services and standards globally? Ms Benn talked about the size of and coverage of Microsoft globally and how its users experience 600 million cyber attacks each day. She said they operate a principles-based approach with privacy as a fundamental human right, irrespective of any privacy protection legislation being in place, and take into account the differences in laws

and culture across the world in terms of service provision and build them in such a way that users can trust them and be safe. She sees the role of Microsoft as encouraging best practice in responsible AI use across the world.

Ms Denham asked Mr de Champris to talk about the EU and the challenges EU members are facing. He said the world was on the cusp of an AI revolution and that Europe cannot afford to be stuck in technologies, centuries and industries of the previous century. He said it was fundamental for Europe to innovate and integrate AI and talked about the complex and inconsistent patchwork of legislation and practice in Europe making it difficult for companies to innovate and integrate AI into their business development. He said that DPAs and other regulators of other policy domains need to collaborate to avoid legal uncertainty. Sensible, pragmatic and flexible interpretations of regulations are what is needed.

Ms Denham questioned whether DPAs have the right skills and capacity, and whether their remit should extend beyond data protection. She asked Ms Benn if she thought DP and AI regulation are aligned or in conflict, and can we extend our view. At a high level, Ms Benn agreed they were aligned and the goal of regulating AI should be to ensure its use is safe.



Chat

The impact of AI

Ms Denham asked Ms Akuetteh and Ms Wimmer if they had a vision of how to be regulators in a world of advanced analytics and the expectations of the changing world. Ms Wimmer agreed that DPAs would need to shift their view to extend beyond personal data and have a broader perspective. DPAs would need greater expertise and more resources to tackle those challenges and changes. Ms Akuetteh believed there is room to build a vision of what the future looks like for regulators and agreed with the need to build capacity of regulators. Regulators need to be open-minded and engage a lot more with technologists and data scientists.

Mr de Champris wants to see regulators embrace more flexible and more risk-based approaches through continuous dialogue with industry. Ms Benn favoured greater partnership across industry and regulators, including civil society and Government, that sees better education for users.

Ms Denham asked if international instruments, such as OECD, Convention 108 and G7 are still of value. Ms Wimmer admitted struggling to keep up and would value a common set of principles or a consensus on them all at an international level. Mr de Champris stated that regulators, policymakers, civil society, companies and industry are all incentivised in implementing AI responsibly. Ms Benn believes that the users will have the biggest voice, because if the technology is not used then there's no utility. Ms Akuetteh was of the view that people do not feel in control because they don't understand the technology.

Key Outcomes:

- A plethora of new laws are creating cross-regulatory tensions.
- DPAs are lacking sufficient skills, expertise, capacity and resources globally.
- Fundamental for Europe to innovate and integrate AI
- Complex and inconsistent patchwork of legislation and practice in Europe making it difficult for companies to innovate and integrate AI into their business development
- Too many international instruments make for a complex regulatory environment. A common set of global principles would be favourable.

Action Points:

- DPAs needed to be agile to respond to user demand for new technologies.
- Collaborate more!
- Sensible, pragmatic and flexible interpretations of regulations.
- DPAs need to broaden their view to extend beyond personal data.





SESSION 2 – INDIVIDUAL



KEYNOTE SPEECH

Douglas Kruger, International Speaker and Business Author

“Who Cares About One Person? How Elevating the Individual Elevates all Humanity.”

Douglas began by emphasising the importance of safeguarding individual interests and questioned the significance of prioritising the individual over the group. He provided an example of a common belief system, “The rich are getting richer,” and debunks it with data from his book “Poverty Proof” stating that the poor are getting richer faster than at any other point in human history.

Douglas discussed the trend of human systems becoming more complex over time, leading to a contraction of human freedom. He highlighted the experiment in Argentina to strip away excess bureaucracy and its significance in the context of species-level trends. He went on to emphasise the global impact of cultural innovations and their ripple effects on human flourishing, introducing the concept of the individual and its historical significance, tracing it back to the ancient Hebrews and the idea of being “made in His image.”

Douglas explained the radical shift in thinking that occurred when humans were seen as inherently special and dignified, rather than tools of the King. He described the historical context of the 13th century, including the rise and fall of empires and the role of English common law in protecting individual rights. This included providing an example of how English common law’s independence from the King led to the unique layout of London and its prosperity, and how this had a long-term impact on British law and society, including the abolition of slavery and the influence on the United States.

Douglas traced back the influence of the idea of individual rights to the American Revolution and the drafting of the U.S. Constitution. He highlighted the unique aspect of the

U.S. Constitution, which protects individual rights and limits the power of the state. He went on to describe the meteoric rise of American prosperity and innovation as a result of this foundational principle, emphasising the unintended consequences of this idea, which lead to unprecedented material gain and the liberation of human talent.

Douglas concluded his keynote by connecting the historical developments to this conference, emphasising the importance of protecting individual rights. He encouraged participants to consider the potential impact of their actions on human talent and potential, and highlighted the global nature of the conference and the diverse cultural contributions to the project of human flourishing. Douglas concluded with a call to action, urging participants to uphold individual rights and contribute to the well-being of the species.

Key Outcomes:

- There is a trend of human systems becoming more complex over time, leading to a contraction of human freedom.
- The global impact of cultural innovations and their ripple effects on human flourishing.
- If you want innovation and prosperity, humans should be seen as inherently special and dignified, rather than tools of the State.

Action Points:

- Consider the potential impact of your actions on human talent and potential.
- Uphold individual rights and contribute to the well-being of the species.

SESSION 2 – INDIVIDUAL



PANEL DISCUSSION (WITH A DIFFERENCE):

The importance of hearing the voices of our next generation cannot be underestimated. In this session we will hear from a group of young people who form part of Jersey's Youth Assembly. They will be discussing "The Privacy Debate: What the Next Generation Think - Defining Privacy Harms: Perspectives on cyber bullying, facial recognition and what privacy means for future generations."

MODERATOR:

Paul Breitbarth (Jersey Data Protection Authority)

PANELLISTS:

4x Hautlieu students

Paul Breitbarth introduced the panel, all digital natives from diverse backgrounds and subjects of study and emphasizes the importance of discussing digital rights and data protection with teenagers. He highlighted the resolution from Mexico in 2021 which focuses on limiting online tracking of children and better education on privacy. He also mentioned the personal data protection competency framework for school students established in Marrakech in 2016.

Initial Thoughts on Privacy

Our speakers discussed the importance of privacy and the challenges of understanding privacy policies when downloading apps. They emphasised privacy as a basic right and the

difficulty of controlling what is shared online, especially with the development of social media and AI.

Two of our panellists agreed on the difficulty of managing personal data from a young age and the lack of control over how information is shared. One of the group added that young people often underestimate the amount of information they post online, which can put them in danger.

Social Media Usage and Privacy Concerns

Paul Breitbarth shared statistics from the Eurobarometer and Pew Research Centre on social media usage among different age groups. The panellists discussed their daily social media usage, with two saying they spent about three hours, another around four hours, and one as much as six hours.

Two panellists talked about checking privacy settings and being aware of how their data is used, such as Instagram being linked to Meta. Some panellists also mentioned having their accounts private but still being concerned about how their information is used.



Impact of Social Media on Mental Health

Paul Breitbarth referenced a report from the US Surgeon General on the benefits and risks of social media use for adolescents. Two of the panellists discussed the negative impact of social media on mental health, including shorter attention spans and lack of sleep, and suggested the need for social media detoxes to reflect on one's behaviour and well-being. The remaining panellists shared experiences of seeing people on their phones instead of engaging in social activities, highlighting the addictive nature of social media.

School Policies on Phone Use

Paul Breitbarth asked the students about school policies on phone use during school hours. One panellist explained that phones are allowed outside classes for accessing online resources but not during class time. Other panellists compared their experiences at different schools, with some schools banning phones outright and others allowing limited use. The panellists discussed the benefits and drawbacks of these policies, including better communication and reduced bullying.

Cyberbullying and Online Safety

One of the panellists shared an incident of cyberbullying involving a friend and the challenges of dealing with inappropriate comments on social media. Others discussed the anonymity provided by online platforms, which can encourage bullying behaviour.

Paul Breitbarth and one of the panellists talked about the importance of understanding the context of online comments and the difficulty of controlling online behaviour, while another mentioned the lack of up-to-date education on online safety in schools, emphasizing the need for regular updates on digital literacy.

Final Thoughts and Recommendations

One panellist emphasised the importance of considering the experiences and opinions of young people when making decisions about social media policies, whilst another argued against a general ban on social media for under-16s, highlighting the need for individual consideration of different circumstances.

Two panellists called for more education on privacy and the importance of understanding how personal data is used online. The session concluded with a call to action for regulators to start talking to the younger generations and not just about them.

Key Outcomes:

- Young people see privacy as a basic right but have difficulty controlling what is shared online.
- Young people often underestimate the amount of information they post online.
- Be mindful of the negative impact of social media on mental health, attention spans, sleep and social relationships
- Anonymity provided by online platforms can encourage bullying behaviour.

Action Points:

- More education on privacy and online safety is needed in schools, including regular updates on digital literacy.
- Regulators need to start talking to the younger generations and not just about them.

SESSION 2 – INDIVIDUAL

PARALLEL SESSION 1



DATA PROTECTION AND MENTAL HEALTH

The session on data protection and mental health in Jersey focused on the balance between individual privacy and collective benefits in health data sharing. Panellists discussed regulatory challenges, including cases like GoodRx and BetterHelp, where sensitive health data was misused for advertising. Alvaro Bedoya highlighted the need for scrutiny of standardized data-sharing practices. Wojciech Wiewiorowski emphasized the fragmented nature of mental health data regulation in Europe. Dan Holloway raised ethical concerns about inferences from mental health data and the importance of user involvement in app design. The discussion also touched on the potential benefits of data sharing, such as personalized treatment plans and informed policy making, while stressing the need for transparency and user control over their data.

MODERATOR:

Advocate Davida Blackmore, Principal (AdvocateDVB) and Chairman of the Mental Health Review Tribunal (Jersey).

PANELLISTS:

- Alvaro Badoya, Commissioner, Federal Trade Commission,
- Wojciech Wiewiorowski, European Data Protection Supervisor
- Dan Holloway, CEO & founder, Rogue Interrobang



The session focused on the sharing of health data, particularly mental health, and the balance between individual privacy rights and collective benefits.

Advocate Blackmore invited the panellists to discuss the challenges of data sharing from a regulatory perspective. Alvaro Bedoya discussed two cases: GoodRx and BetterHelp, highlighting issues with data being shared with third parties for advertising purposes. A totally different purpose from what is what collected for. He highlighted the trend among third party advertisers that assumes just because the sharing may be a standard practice, but not necessarily legal. Alvaro emphasized the need to scrutinize the advertising ecosystem when dealing with sensitive health information.

Wojciech Wiewiorowski discussed the legal and ethical concerns regarding data sharing, noting the diverse legislation and fragmented information in Europe. He said that the EDPS has to sometimes go out of its typical role of data protection regulation into privacy matters. He also noted that not all data about mental health is treated the same way.

In terms of the legal and ethical concerns, Wojciech again highlighted the diverse legislation and fragmented information in Europe (largely due to different ideologies of medical health), making it difficult for researchers. Alvaro mentioned the legal framework in the US, citing relevant sections of the FTC Act and the Health Breach Notification Rule. Dan Holloway raised ethical concerns about inferences made from mental health data and the lack of transparency in how those inferences are used and how data is used. He shared a story about the importance of context in data sharing and the role of inference, comparing it to choosing a carpet shade. Dan was of the opinion that too much automatic assumption that information about mental health is useful often that means that it's useful to the company and not to the consumer.

Wojciech commented on the benefits and challenges of data sharing, including personalised treatment plans, scientific collaboration, and informed policy making. Advocate Blackmore mentioned the potential for apps to be prescribed by doctors in Germany, raising concerns about privacy and consent. Dan expressed scepticism about the benefits of apps, emphasising the need for co-production and user involvement in design, and Alvaro discussed the importance of scientific validation before assuming benefits of new technologies.

In respect of increasing trust, Dan emphasised the need for user involvement in the design of apps and the importance of co-production. Alvaro discussed the challenges of capacity and the need for regulators to upskill and collaborate with NGOs. Wojciech highlighted the importance of cooperation with NGOs and the role of self-certification in Australia and stated that without their help we are blind. Dan raised concerns about the ease of changing or withdrawing data, emphasising the need for practical solutions.

Key Outcomes:

- Third party advertisers are assuming that just because the sharing may be a standard practice, it is legal to do so. But that may not necessarily be the case.
- Diverse legislation leads to fragmented information in Europe, due to different ideologies of medical health.
- Not all data about mental health is treated the same way.
- There is a lack of transparency in how inferences made from mental health data are used. It might be useful to the company, but at the same time a risk to the individual.
- There is scepticism about the benefits of prescribed (and unprescribed) apps, and there is a need for co-production and user involvement in design.
- Capacity issues amongst DPAs means that collaboration with NGOs is essential.

Action Points:

- Investigate the use of self-certification schemes for mental health apps to provide more transparency and user reassurance.
- Explore ways to make it easier for individuals to change their mind and withdraw sensitive mental health data that has been shared.
- Build out a behavioural science team at the regulatory body to better assess the potential harms and benefits of platform design and data sharing practices.
- Increase cooperation between data protection authorities and NGOs to stay informed about emerging technologies and their impact on mental health.

SESSION 2 – INDIVIDUAL



PARALLEL SESSION 2

DEFINING PRIVACY HARMS IN A MODERN WORLD

This discussion focused on defining and mitigating privacy harms in the digital age. Bojana Bellamy emphasised the need for systematic, consistent frameworks to measure and address these harms. Anu Talus highlighted the General Data Protection Regulation's risk-based approach, while Emily Keaney discussed the importance of accountability and balancing risks with benefits. Andy Phippen raised concerns about youth privacy and the role of education. Jade Nester from TikTok detailed their risk assessment processes, including user feedback and collaboration with safety advisory councils. The panel agreed on the importance of transparency, accountability, and the need for a holistic approach to digital harms, emphasising the balance between privacy, safety, and societal benefits.

MODERATOR:

Bojana Bellamy

PANELLISTS:

- Anu Talus, Chair, European Data Protection Board
- Emily Keaney, Deputy Commissioner, UK ICO
- Andy Phippen, Professor, Bournemouth University
- Jade Nester, Head of Data Public Policy, Europe, Tik Tok

Bojana Bellamy introduced this session on defining privacy harms, emphasising the importance of systematic and consistent measurement. She reflected on the evolution of privacy harms discussions since 2014 and questioned whether progress has been made in defining and measuring privacy harms.

The discussion expanded to include broader digital harms, such as online safety and cybersecurity and the need for a holistic approach to harms. Bojana outlined the three fundamental ways the Centre for Information Policy Leadership believes laws should be based on harms: higher regulation in high-risk areas, accountability in everyday practices, and strategic consideration by regulators.

Anu Talus discussed the GDPR's focus on risk rather than harm, and how risk shapes legal obligations for data controllers. She explained the role of data protection authorities in dealing with complaints and allocating resources based on risk. Emily Keaney emphasised the importance of accountability and the need for organisations to consider potential risks to individuals. She highlighted the role of regulators in allocating resources based on the greatest risks and potential harms and the importance of empowering organisations to use data in beneficial ways.

Andy Phippen provided an academic and industry insight into privacy harms. He reflected on his work with young people and the lack of focus on education around digital rights and privacy, and shared examples of how young people's privacy is often compromised by stakeholders closer to them, such as foster care teams and schools.

Jade Nester from TikTok discussed the company's extensive consultation process and the importance of user feedback in assessing and mitigating harms. She talked about the need for collaboration between privacy and safety teams within companies to address both privacy and online safety harms.



Bojana and Emily discussed the challenges of measuring and mitigating privacy harms, including the difficulty of defining and proving harm. Emily highlighted the importance of accountability and the role of regulators in ensuring organisations take responsibility for mitigating risks. Andy emphasised the need for critical education around digital rights and the relationship between users and platforms. All panellists discussed the importance of transparency and user empowerment in addressing privacy harms.

The panellists discussed the balance between privacy and benefits in data processing, with Emily suggesting the need to consider both risks and opportunities. Jade shared examples of how TikTok has implemented features to support user autonomy and provide guardrails for safe and beneficial use of the platform. Anu highlighted the importance of strategic priorities in data protection authorities and the need to focus on the most significant risks. All agreed on the importance of considering the broader implications of data processing and the need for a holistic approach to privacy and safety.

The audience raised questions about the challenges of demonstrating harm and the importance of addressing manipulation in data processing, and the need to include members of the public in our discussions, ie those who are being impacted. Are they experiencing 'harms'?

Jade talked of the importance of user feedback and ongoing research to continuously improve and address potential harms, while Emily discussed the role of regulators in considering economic growth and the importance of balancing competing rights and demands. Andy highlighted the need for critical education and transparency to empower users and address the broader implications of data processing.

In terms of next steps, Bojana summarised the key points of the discussion, emphasising the need for accountability, transparency, and collaboration in addressing privacy harms. The panellists agreed on the need for ongoing research, user feedback, and strategic priorities to continuously improve and address potential harms. The session concluded with a call to action for organisations and regulators to take ownership of understanding and managing privacy harms.

Key Outcomes:

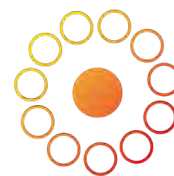
- A holistic approach with systematic and consistent measurement is needed when defining privacy harms. Harm is difficult to prove.
- The role of regulators is to allocate resources based on the greatest risks and potential harms, while empowering organisations to use data in beneficial ways.
- There is still a lack of focus on education around digital rights and privacy amongst children.
- There is a need for collaboration between privacy and safety teams within companies to address both privacy and online safety harms.
- Demonstrating harm is challenging. It is important to address manipulation in data processing and discussions must include those who are being impacted.

Action Points:

- Explore a unified approach to risk assessment that considers both privacy and online safety.
- Continue multi-stakeholder discussions on topics like age assurance to address overlapping privacy and safety concerns.
- Increase transparency around reporting and addressing of harmful content.
- Enhance digital literacy and empower users to take more responsibility in curating their online experiences.
- Ongoing research, user feedback, and strategic priorities are required to continuously improve and address potential harms.
- Organisations and regulators to take ownership of understanding and managing privacy harms.



SESSION 3 – INDEPENDENCE



KEYNOTE SPEECH

Marie Laure Denis, President, CNIL

“How Technology Will Impact the Regulator: What does our future as digital regulators look like?”

President Denis started by suggesting that making sure data protection authorities can handle technological developments has always been important to decision-makers. Discussions during the 1978 debates on the IT and Freedom law show that the supervisory authority should apply knowledge to technology, have technical skills, and engage with the outside world. She emphasised that Independence is vital for its effectiveness.

She said that the future data protection authority will adapt to the presence of digital technologies in society. The regulations are designed to be technologically neutral, ensuring they endure over time. She described how the CNIL has evolved significantly, adapting to technological changes and collaborating with other regulators, focusing on improving the protection of people's rights through better compliance.

President Denis said it is crucial to understand and have expertise in the financial impact of these technologies. She said that the CNIL uses legal-engineer pairs to ensure effective investigations and have established an artificial intelligence department to clarify rules and promote responsible innovation. Amongst other initiatives, they created a digital innovation laboratory to maintain a connection with technology trends and regularly shares its findings through publications. She said that digital technologies are evolving rapidly, and we need to anticipate and understand these changes.

President Denis described the importance of having technical expertise in house to navigate a new economic model focused on data exploitation and behavioural advertising, supported by advancements in artificial intelligence, quantum technologies, and neurotechnologies. She acknowledged the importance of outside reading to help in understanding technology and applying regulations better. Engagement with data processing organisations allows for effective dialogue, supported by tools developed over the years to support companies and help them towards compliance.

She discussed how regulation helps identify the level of compliance maturity within a sector. Additionally, it is essential to function within a collective of digital regulators, considering the international nature of data flows today. Moreover, cooperation among data protection authorities is vital as regulatory boundaries are becoming more complex, especially in the European Union, where multiple regulations have been adopted.

President Denis discussed how the CNIL places an emphasis on privacy by design, including introducing a sandbox to assist a hospital in using federated learning for clinical studies. They have also worked on a prototype to block minors from accessing adult content without compromising privacy by using cryptographic techniques. She said that new technologies may enhance CNIL's daily work, leading to discussions on how to utilise these tools effectively, and highlighting the need to keep up with rapid technological changes and strengthen cooperation.



Key Outcomes:

- DPAs must be able to handle technological advancements and adapt accordingly.
- Collaboration with other DPAs and technology processors is critical for future success.
- DPAs must include technical expertise within their offices to properly understand the impact of new technologies.

Action Points:

- Explore the use of new technologies within DPAs to help manage a complex environment.

SESSION 3 – INDEPENDENCE



PANEL DISCUSSION: “REGULATORY COUSINS”

The panel discussed the increasing complexity of global privacy and digital regulations, highlighting a significant rise from 10% to 79% of the world’s population now covered by comprehensive national privacy legislation in just four years. Key points included the need for a global, integrated regulatory system, outcome-based collaboration, and the importance of context and culture in addressing regulatory challenges. Examples from OpenAI and GSMA illustrated the practical implications of these complexities, emphasizing the need for adaptive regulations and digital diplomacy. The discussion concluded with a call for new energy to combat regulatory entropy and improve regulatory cohesion.

MODERATOR:

Trevor Hughes, CEO, the IAPP

PANELLISTS:

- Christopher Hodges OBE, Chair, Regulatory Horizons Council; Emeritus Professor of Justice Systems, Oxford University
- Noriswadi Ismail, Senior Director for Data Privacy, GSMA
- Thibault Schrepel, Associate Professor of Law at the Vrije Universiteit Amsterdam, Faculty Affiliate at Stanford University
- Emma Redmond, Open AI

Trevor Hughes introduced the panel and highlighted the importance of the topic: Regulatory complexity and the challenges faced in the current moment. He provided a brief overview of the panel’s agenda and shared a statistic from Gartner, indicating that 10% of the world’s population was covered by national privacy legislation before the pandemic, increasing to 79% in just four years, highlighting the rapid growth in privacy legislation globally.

Trevor emphasised the diversity of privacy standards, noting that they are not all based on the GDPR and that there are differing definitions and standards on data transfers. He mentioned the EU AI Act and its complexity, pointing out that it references over 40 other digital policy directives and standards within the EU. Trevor discussed the broadening of the IAPP’s mission to cover AI governance, cybersecurity law, and digital responsibility, highlighting the need for councils and committees to ensure cohesion of digital policy issues, consistency and recognition of overlaps. Trevor pointed out that the title of privacy leaders inside organisations has evolved, with many now having additional responsibilities.

Christopher Hodges discussed the pace of technological change and the inadequacy of existing regulatory mechanisms to keep up. He argued that law is not the sole solution, and that a global, integrated system is needed to address the challenges posed by global technologies. Christopher emphasised the importance of behavioural psychology and sociology in understanding and addressing regulatory challenges, proposing outcome-based collaboration as a solution, and highlighting the need for a collaborative culture and psychological safety.



Emma Redmond discussed the complexity of managing multiple overlapping regulatory demands at OpenAI. She talked about the importance of collaboration and a culture that demands agility and contextual thinking and provided examples of OpenAI's projects, such as Digital Green, Madea, Color Health, and Be My Eyes, to illustrate the benefits of AI. Emma highlighted the need for a culture that fosters human-to-human interaction and collaboration to address regulatory challenges effectively. Noriswadi Ismail discussed the regulatory challenges faced by GSMA members, particularly in emerging markets. He highlighted the importance of understanding local cultures, traditions and customs in different jurisdictions, providing examples of regulatory concerns, such as network shutdowns and taxation on personal data, and the need for contextualized solutions. He emphasised the importance of digital diplomacy and thinking outside the box to address regulatory challenges effectively.

Thibault Schrepel discussed the challenges of AI and competition law, highlighting the trade-offs between competition and privacy. He provided examples from the AI Act, such as the tension between transparency, data protection and antitrust infringements. Thibault emphasised the need for computational tools to detect and document regulatory tensions and the importance of policy makers developing compliance checks. He concluded with the idea that policymakers should use technology to better understand and address regulatory challenges.

Trevor summarised the panel's discussion, emphasising the need for new energy to combat regulatory complexity and chaos. The panellists provided final recommendations: Emma emphasised the importance of context, Noriswadi suggested thinking outside the box, and Thibault highlighted the need for adaptive regulation and digital diplomacy.

Key Outcomes:

- The global coverage of data protection legislation around the world has risen by 69% in four years.
- There is a diversity of privacy standards, complexity in application and a need for cohesion in digital policy issues.
- Existing regulatory mechanisms cannot keep up. A global, integrated system is needed to address the challenges posed by global technologies.
- Businesses are struggling to navigate the complexity of managing multiple overlapping regulatory demands.
- Understanding local cultures, traditions, and customs in different jurisdictions is crucial to addressing regulatory challenges effectively.
- Policymakers should use technology to better understand and address regulatory challenges.

Action Points:

- Explore outcome-based collaboration models that leverage behavioural science and technological platforms to address regulatory challenges.
- Develop a culture of collaboration and contextual problem-solving within organisations to navigate the complex regulatory landscape.
- Advocate for digital diplomacy and consider 'thinking outside the box' to address the present and future state of digital regulation.



SESSION 4 – INTERNATIONAL



PANEL DISCUSSION: “THE ADVANTAGES AND CHALLENGES OF DATA TRANSFER TOOLS”

MODERATOR:

Joe Jones, Research Director, the IAPP

PANELLISTS:

- Clarisse Girot, OECD
- Estelle Masse, European Commission
- Commissioner Asai, Japan PPC
- Haksoo Ko, Chairperson, PIPC Korea

The discussion focused on international data transfers and the complexities of privacy compliance. Key panellists included Estelle Masse from the European Commission, Commissioner Asai from Japan, Chairperson Ko from Korea, and Clarisse Girot from the OECD. They highlighted the importance of trusted data flows and the evolving mechanisms for data adequacy, such as mutual adequacy decisions with Japan and the UK and ongoing assessments with Brazil and Kenya. The conversation also covered the challenges of contractual clauses, binding corporate rules, and certification schemes, emphasising the need for practical, implementable solutions to ensure safe and trusted data transfers.

Joe Jones introduced the panel and spoke about the importance of international data flows and the complexity of privacy issues they entail.

Commissioner Asai emphasised the importance of data free flow with trust and mentioned Japan's engagement with adequacy arrangements and certification mechanisms. He highlighted Japan's readiness to apply a draft resolution in upcoming management meetings and expressed interest in exchanging opinions on different approaches. Joe underscored the significance of the concept of data free flow with trust, introduced by the late Prime Minister Shinzo Abe.

Estelle Masse discussed the European Union's priority of advancing safe and trusted data flows and the importance of protection travelling with the data. She explained the dual goal of ensuring individual protection and providing legal certainty for business operators and researchers, emphasising the need for adaptable regulation to accommodate diverse markets and actors, and highlighting the convergence and evolution of data flow tools.

Chairperson Haksoo Ko outlined two general philosophies: Supporting international data flows and ensuring trustworthy data governance regimes. He spoke about the complexity of data-related issues and the need for a set of different mechanisms tailored to specific circumstances. Chairperson Ko discussed the importance of interoperability and harmonisation among different data transfer schemes.



Clarisse Girot shared her experience working with the Jersey Data Protection Authority and emphasised the importance of trust in cross-border data flows. She explained the OECD's role in gathering insights from industry stakeholders, regulators and civil society to support trusted data flows. She also highlighted the importance of regulatory cooperation, transfers of non-personal data, and privacy-enhancing technologies in facilitating trusted data flows.

Joe asked Estelle to discuss the advantages and challenges of data adequacy. She explained that adequacy is a comprehensive and significant mechanism for integrating economies and ensuring data protection, citing the EU's mutual adequacy decisions with Japan, the UK and ongoing discussions with Brazil and Kenya. Estelle also highlighted the importance of adequacy in facilitating data flows and the need for continuous review and updates.

Joe asked Commissioner Asai about Japan's priorities and perspectives on data adequacy and equivalency. He outlined the advantages of adequacy, including the energy and effort required for assessments and the benefits for enterprises. He also emphasised that the work is done by policymakers and companies benefit from the list of adequate jurisdictions. Chairperson Ko explained Korea's approach to equivalency and the mutual assessment process with the EU and the UK.

Joe asked Estelle to discuss the advantages and challenges of contractual clauses. Estelle explained the convergence of contractual clauses globally and the importance of making them interoperable. Joe then asked Clarisse about Binding Corporate Rules (BCRs) and certification schemes. Clarisse emphasised the importance of making tools like BCRs and certification schemes practical and implementable.

Joe asked Commissioner Asai about Japan's interest in the Global Cross-Border Privacy Rules (CBPR) system. The Commissioner explained the advantages of the CBPR system for ensuring data protection within companies. Joe asked Chairperson Ko and Clarisse to add their perspectives on certification schemes. Both emphasised the need for practical implementation and business demand for certification tools.

In conclusion, Joe reiterated the importance of trusted data flows and the need for continued collaboration and innovation in this field.

Key Outcomes:

- It is priority of the European Union to advance safe and trusted data flows and the importance of protection travelling with the data.
- There is a need for a set of different mechanisms tailored to specific circumstances, with interoperability and harmonisation a key component among different data transfer schemes.

- Privacy-enhancing technologies are needed to help facilitate trusted data flows.
- Adequacy is a comprehensive and significant mechanism for integrating economies and ensuring data protection.
- Tools like BCRs and certification schemes need to be practical and implementable.

Action Points:

- Explore the possibility of mutual adequacy assessments between the EU and other jurisdictions like Brazil, Kenya, and Korea.
- Assess the EU's data protection law for potential equivalency with Korea's data protection regime.
- Revisit the design and implementation of Binding corporate rules to make them more practical and globally applicable.
- Encourage more companies to participate in certification schemes like the APEC Cross-Border Privacy Rules (CBPR) system to increase adoption.

SESSION 4 – INTERNATIONAL



PANEL DISCUSSION: “INTERNATIONAL TRANSFERS IN THE CONTEXT OF FINANCIAL SERVICES - WHAT IS THE DIRECTION OF TRAVEL? WHAT DOES THE FUTURE LOOK LIKE FOR DATA TRANSFER MECHANISMS?”

Moderator:

Vivienne Artz, Founder of Picasso Awards and Advisor to the Centre for Information Policy Leadership.

Panellists:

- Lori Baker, Dubai International Finance Centre
- Jill Britton, Director General, Jersey Financial Services Commission
- Katherine Race Brin, CDPO, World Bank

The discussion on international transfers in financial services highlighted Jersey's significant role, with financial services contributing 40% directly and up to 70% indirectly to its economy. Key panellists from the Jersey Financial Services Commission, World Bank, and Dubai International Financial Centre emphasised the critical need for data transfers in financial services, noting that data flows are essential for global transactions, anti-money laundering, and financial crime prevention.

The conversation also covered the importance of data minimisation, privacy-enhancing technologies, and the challenges of aligning financial services regulation with data protection laws. The panellists stressed the necessity of global standards and mechanisms to facilitate data transfers while ensuring privacy and security.

Vivienne Artz introduced the topic of international transfers in financial services, emphasising their importance to Jersey's economy. She shared the historical significance of Jersey, including the discovery of 70,000 Celtic coins and the establishment of the first bank in 1796. She went on to highlight Jersey's modern financial services industry, which is about 63 years old, and mentions the island's famous exports like Jersey Royal potatoes and Jersey milk. Vivienne discussed the essential role of data transfers in financial services, emphasising their impact on personal, business, and trade activities. She discussed the shift towards digital and global financial services, noting the increasing complexity and diversity of the sector, and explained the importance of instantaneous data flow for the proper operation of economies and the provision of financial services.

Vivienne invited Jill Britton to provide a deeper dive into Jersey's financial services sector and the range of organisations it regulates. Jill explained the global and local economic contributions of financial services, noting that it accounts for 40% of Jersey's GDP directly and up to 70% indirectly. She outlined the breadth of services offered in Jersey, including traditional banks, private banks, investment banks, trust companies, and non-traditional financial services like lawyers and accountants. Jill mentioned the significant customer base and payment distribution of Jersey's financial services sector, which spans 233 countries, and discussed the complexity of financial services transactions, involving multiple parties and the need for data flow between them.

Katherine Race Brin from the World Bank discussed the importance of data transfers for the bank's mission, including direct lending, consulting, and policy work. She spoke about the bank's privacy program, which includes principles like legitimacy, consent, accuracy, transparency, and accountability. Katie expressed concerns about proposed frameworks that could impede data transfers to international organisations, emphasising the need for flexibility. Vivienne and Katherine discussed the structured nature of data flow in financial services, using SWIFT messages as an example and the importance of corresponding banking arrangements.

Lori Baker explained the evolution of Dubai's financial services sector, including the establishment of the Dubai International Financial Centre and the DIFC Data Protection Law. She described the close collaboration between the Dubai Financial Services Authority and the Office of the Commissioner for Data Protection and discussed the updates to Dubai's data protection law in 2020 and the importance of balancing data protection with financial crime prevention. Lori highlighted the challenges of implementing non-financial services regulations and the ongoing efforts to ensure compliance and protect data.

Vivienne and Jill discussed the importance of global data sharing between regulators to combat financial crime and ensure the integrity of financial services. Jill mentioned the role of IOSCO and MOUs in facilitating data sharing between regulators and the critical need for information exchange in the fight against financial crime.

Vivienne emphasised the evolving nature of financial services and the need for mechanisms that can adapt to new technologies and business models. The panellists discussed the importance of trusted relationships and the use of technology to support data transfers while maintaining privacy and security.

Lori introduced the Ethical Data Risk Index, a guidance tool to assess the safety of data transfers based on various thematic areas. She explained the six thematic areas covered by the index, including laws and regulations, privacy culture and government access to data. She highlighted the importance of the index as a guide for organisations to assess the risks associated with data transfers and make informed decisions. The panellists discussed the potential for the index to evolve into a multilaterally agreed framework for data transfers.

Katherine suggested data minimisation and pseudonymisation as effective tools for protecting data while facilitating transfers. She acknowledged the challenges of implementing privacy-enhancing technologies in developing countries and the need for pragmatic solutions. Jill called for closer alignment between financial services regulation and data protection legislation to reduce complexity and challenges. The panellists discussed the need for a global standard that is principles-based rather than prescriptive to support the evolving nature of financial services.

To summarise, Vivienne revisited the key points discussed, emphasising the importance of data transfers in financial services and the need for trusted relationships and technology. She highlighted the importance of protecting customer data while ensuring the integrity of financial services systems.

Key Outcomes:

- Data transfers have an essential role in financial services, with significant impact on personal, business, and trade activities.

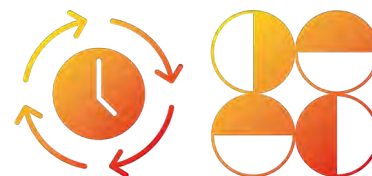
- Optimum operation of economies in the provision of financial services requires instantaneous data flow.
- Proposed data transfer frameworks could impede data transfers to international organisations, therefore there is a need for flexibility in these proposals.
- Global data sharing between regulators to combat financial crime and ensure the integrity of financial services is essential.
- Financial services is constantly evolving and requires mechanisms that can adapt to new technologies and business models.
- Tools such as Dubai's Ethical Data Risk Index can be used as a guide for organisations to assess the risks associated with data transfers and make informed decisions.
- Pragmatic solutions are needed to address the challenges faced by developing countries in implementing privacy-enhancing technologies.
- A principles-based global standard is needed to support the evolving nature of financial services.

Action Points:

- Explore the development of a global, principles-based standard for data transfers in financial services to reduce complexity and challenges.
- Investigate the use of privacy-enhancing technologies, such as federated identity and pseudonymisation, to enable secure data transfers, particularly when working with parties with varying levels of resources.
- Continue to strengthen the collaboration and alignment between financial services regulators and data protection authorities to ensure the effective and compliant flow of data.



SESSION 5 – INDIGENOUS & INTERCULTURAL



KEYNOTE SPEECH

Massimo Marelli, Head of the Data Protection Office at the International Committee of the Red Cross
“The Role of Data Privacy in Humanitarian Crises”

Massimo Marelli, with 11 years of experience in data protection and privacy at the International Committee of the Red Cross (ICRC), emphasised the critical role of data protection in humanitarian contexts. Highlighting the ICRC’s operations in conflict zones, he argued that data protection is not just compliance but safeguards individual dignity and agency. He discussed the challenges of applying data protection principles in areas without legal frameworks, using examples like consent for restoring family links in conflict zones. The ICRC has collaborated with organisations like the IFRC and the UNHCR to develop practical guidelines and training programs, training over 4,500 practitioners globally.

Introduction and Background

Massimo described how the ICRC’s mandate is derived from international humanitarian law, including the Geneva Conventions and laws of war. It operates in volatile environments, including conflicts in Gaza, Lebanon, Ukraine, Sudan, Yemen, South Sudan, Congo, and Syria. He talked about the importance of data protection in humanitarian contexts, describing it as a privilege and a fundamental aspect of safeguarding individual dignity.

The Essence of Data Protection

Massimo argued that data protection is not just a compliance exercise but a fundamental aspect of humanity, safeguarding individual dignity and enabling agency. Data protection ensures accountability and transparency for organisations handling personal information. He described it as a useful tool for humanitarian organisations, helping to apply the principle of “do no harm” in complex and volatile environments, and identified that the application of data protection principles varies based on cultural, community and individual factors.



Challenges in Perception and Understanding

Massimo spoke about common misperceptions about data protection, such as it being a compliance exercise or solely about encryption and cybersecurity. He mentioned the confusion people outside the expert community have about data protection, often linking it to navigating privacy policies and cookie banners. He said data protection is often associated with significant fines or data breaches in the news. Rather, the focus should be on its meaningfulness in situations without legal protections, where those protections either don't exist, or are inaccessible. Massimo highlighted the importance of data protection in humanitarian emergencies, where identity and data can lead to persecution, deprivation of freedom or even death.

Data Protection in Extreme Contexts

Massimo explained that data protection is crucial in humanitarian contexts, where legal systems and protections are often eroded or non-existent. He talked about the impact of surveillance and tracking on individuals, emphasising the need for data protection to ensure safety and dignity. He said that data protection is much more than taking care of what happens to data. Rather, it is linked to the capacity to deliver and assist with the safety of individuals, particularly in situations where identity can lead to persecution. He said it is about respecting individual dignity, enabling agency and ensuring transparency and accountability for organisations handling data.

Concrete Examples in the Field

Massimo went on to give an example of a child abducted by a rebel group and the complexities of obtaining consent for restoring family links. He questioned whose consent should be used and the implications of relying on consent in such extreme situations. Massimo believes the example highlights the need for a deep understanding of the principles of lawfulness and fairness, and the context in which they are applied. He said when we talk about personal data protection, we are talking about choices for people that really matter. Choices that will impact their lives and the use of data.

Collaboration and Training Initiatives

Massimo spoke about the collaboration with data protection authorities, privacy commissioners and other humanitarian organisations to develop meaningful applications of data protection principles. He said it highlights the endorsement of the third edition of the guidelines and the development of a training and certification programme with the University of Maastricht, a programme which has held 14 sessions and training for over 500 practitioners from across the globe.

He concluded by saying that data protection is presented as a tool for applying the principle of “do no harm” in an increasingly digital environment, especially in humanitarian settings.

Key Outcomes:

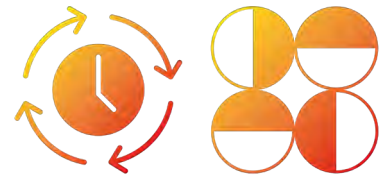
- The perception of data protection is that it is a compliance exercise or solely about encryption and cybersecurity. Data protection is not just a compliance exercise but a fundamental aspect of humanity, safeguarding individual dignity and enabling agency.
- Data protection ensures accountability and transparency for organisations handling personal information.
- The application of data protection principles varies based on cultural, community, and individual factors.
- Data protection is often associated with significant fines or data breaches in the news, instead of focusing on its meaningfulness in situations without legal protections, where those protections either don't exist, or are inaccessible.

- When we talk about personal data protection, we are talking about choices for people that really matter. Choices that will impact their lives and use of their data.
- Collaboration with data protection authorities, privacy commissioners and other humanitarian organisations helps to develop meaningful applications of data protection principles.

Action Points:

- Educate businesses and the wider community to stop thinking of data protection as a compliance exercise and start thinking about it in terms of its meaningfulness in situations where people don't have a voice or cannot use it.
- Be careful to consider the cultural, community and individual factors when applying data protection principles.

SESSION 5 – INDIGENOUS & INTERCULTURAL



PANEL DISCUSSION: “HOW DO INDIGENOUS COMMUNITIES DEVELOP THEIR OWN DATA PROTECTION FRAMEWORKS?”

MODERATOR:

Malcolm Crompton, IIS Partners

PANELLISTS:

- Immaculate Kassait, Commissioner, Kenya ODPC
- Josefina Roman Vergara, Commissioner, Mexico INAI
- Shana Morgan, Global Head of Privacy Compliance, L3Harris Technologies

This discussion highlighted the disparities in data privacy and protection for indigenous communities, emphasising the need for culturally sensitive frameworks. Key points included the challenges of language barriers and the lack of recognition of indigenous rights in many countries. Specific metrics: 6% of the world's population is indigenous, with 10% of Mexico's population identifying as indigenous. The panellists stressed the importance of self-determination, cultural sensitivity, and the need for AI to be used ethically and respectfully. They called for global privacy standards to include indigenous perspectives and for indigenous communities to have a voice in data governance.

Opening Remarks and Introduction to the Panel

Malcolm Crompton started the session by acknowledging his own privilege and reflected on the broader implications of data privacy and protection, particularly for those who do not have the same privileges. He highlighted the lack of discussion on the experiences of original peoples at previous conferences, noting the importance of understanding diverse perspectives. He introduced the concept of colonial settler countries and the damage caused to indigenous populations, urging the audience to feel challenged and confronted by the panel's discussion.

Introduction of Panellists and Initial Questions – Why is your world so different?

Malcolm invited the panellists to share why their world might be different from the audience's world.

Josefina Roman Vergara discussed the cultural and linguistic diversity in Mexico, highlighting the challenges of communication and education for indigenous populations. Shana Morgan, from the Cherokee Nation in the US, emphasised the diversity within indigenous communities and the need for recognition and rights within the broader context of US citizenship. Immaculate Kassait, from Kenya, addressed the lack of recognition of indigenous issues in African contexts and the need for frameworks that adequately protect the rights of indigenous groups.



Challenges and Importance of Indigenous Data Protection

Malcolm asked the panel why it matters to address these issues and what challenges the panellists face in their communities.

Josefina explained the challenges of informing indigenous populations about their rights, particularly due to language barriers and the complexity of Mexico's linguistic diversity. Shana discussed the misconception that indigenous peoples are relics of the past and the need to raise awareness about their thriving cultures and the importance of data control, while Immaculate highlighted the historical harm caused by unauthorised collection of indigenous data and the need for frameworks that respect and protect indigenous beliefs and cultural practices.

Frameworks and Solutions for Indigenous Data Protection

Malcolm asked the panellists for their thoughts on what the Global Privacy Assembly should be doing to address these issues.

Josefina emphasised the importance of shared responsibility and the need for specific laws and regulations to protect indigenous data and Shana called for recognition and a seat at the table for indigenous communities in discussions about data protection and privacy frameworks. Immaculate suggested new principles for data governance that prioritise collective benefits, ethics and ownership for indigenous communities.

Audience Questions and Discussion on AI and Data Protection

One audience member asked about the impact and opportunities of artificial intelligence for indigenous communities, referencing an example of AI being used to reclaim lost languages. Shana discussed the potential of AI in environmentalism and the importance of including indigenous knowledge in AI systems, while also highlighting the risks of misuse and lack of control.

Immaculate emphasised the need for ethical considerations in AI development and the importance of community ownership and control, while Josefina mentioned the use of AI in Mexico's National Transparency Platform and the need for careful implementation to avoid discrimination and ensure accessibility.

Global Regulation and Decolonisation of Data Protection

Another audience member asked if the global application of GDPR is a form of 21st-century colonialism, prompting a discussion on the fit-for-purpose nature of data protection frameworks. Immaculate suggested viewing GDPR as a framework that can be adapted to different cultural contexts and emphasised the need for self-determination in data protection. Josefina highlighted the importance of global standards and

the role of regional networks in creating and implementing these standards. Malcolm and Shana discussed the need for culturally appropriate frameworks and the importance of involving indigenous communities in the development of these frameworks.

Final Thoughts and Closing Remarks

The last question from the audience, a member of parliament from Kenya, raised concerns about the protection of indigenous cultures and morals in the digital age, asking for frameworks that address these issues. Shana emphasised the need for dialogue with indigenous communities to develop appropriate frameworks and highlights the diversity of experiences within indigenous populations.

Key Outcomes:

- There is a lack of discussion internationally on the experiences of original peoples at previous conferences, noting the importance of understanding diverse perspectives.
- There are challenges of communication and education for indigenous populations which need addressing, and a need for recognition and rights within the broader context of citizenship.
- There is a lack of recognition of indigenous issues in many countries and a need for frameworks that adequately protect the rights of indigenous groups.
- Indigenous communities face real harms (current and historical) through unauthorised collection of personal data because those communities are often seen as relics of the past.
- Indigenous knowledge must be included in AI systems, while also highlighting the risks of misuse and lack of control.

Action Points:

- Ensure indigenous communities have a consistent seat at the table in data privacy discussions.
- Develop new principles around data governance for indigenous communities, considering aspects like collective benefits, ethics and ownership.
- Establish a dedicated working group within the Global Privacy Assembly to specifically focus on the challenges and solutions for protecting indigenous data rights.
- Engage directly with indigenous populations within each country to understand their unique cultural contexts and implement appropriate frameworks and legislation.



DAY 3: WEDNESDAY 30TH OCTOBER 2024

SESSION 6 – INDIVIDUAL



KEYNOTE SPEECH

Kate Wright, Director, Arbore Consulting, Co-Founder of the Diversity Network Jersey

“Reducing Inequalities in Privacy Rights: Exploring the different privacy dimensions of diversity.”

Kate Wright, a cultural change specialist and social justice activist, discussed the importance of privacy rights and their impact on diversity. Highlighting her work with the Violence Against Women and Girls Taskforce in Jersey, she revealed that over a third of victim-survivors experienced online abuse, with two-thirds of young people receiving unwanted sexual messages. She emphasised the need for cultural shifts to prioritise data privacy as a human right, addressing biases in data handling, and building trust within communities. She called for inclusive policymaking, transparency and ethical practices to protect the most vulnerable, particularly women and ethnic minorities, from digital exploitation.

as not being a compliance task but rather a safeguarding measure for individuals. She highlighted missed opportunities in corporate culture and understanding of data protection laws and discussed the importance of diversity, equity, and inclusion (DEI) data collection and the barriers to doing so in Jersey.

Barriers to Diversity Data Collection in Jersey

Kate Identified three common barriers to collecting diversity data: ignorance, fear, and trust issues. She explained the unique demographic challenges in Jersey and the lack of compelling reasons for businesses to collate this data, together with a fear of backlash and infringing on data privacy as a significant barrier. She emphasised the need for cultural shifts and leadership to overcome these barriers.

Impact of Privacy Rights on Vulnerable Groups

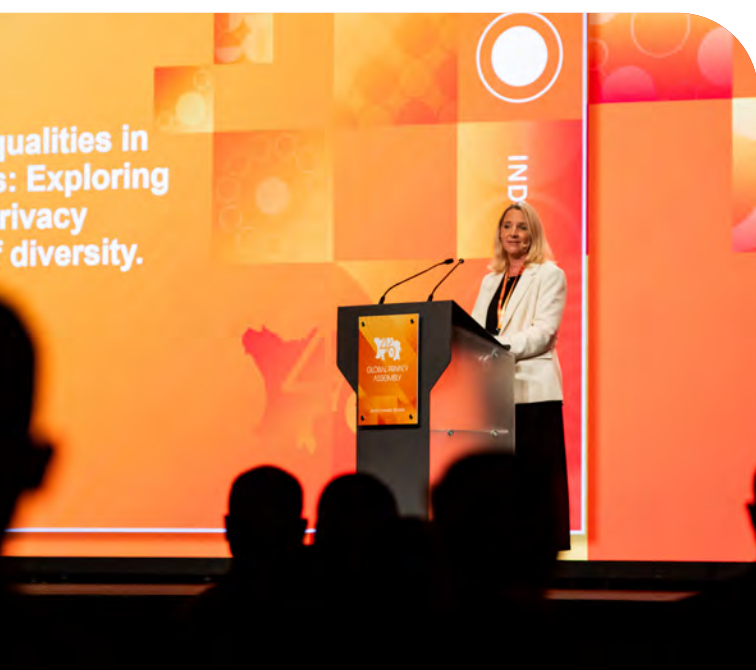
Kate transitioned to community-focused work and the critical role of privacy rights in daily lives, highlighting the uneven impact of data privacy on different demographics, particularly women, children and ethnic minorities. She shared her experiences from chairing the Violence Against Women and Girls Taskforce in Jersey and described the prevalence of gender-based violence and abuse among young women and children in Jersey.

Online Abuse and Privacy Violations

Kate went on to talk about the various forms of online abuse experienced by women and girls, including coercive control, emotional abuse and online harassment. She provided statistics on the prevalence of online abuse in Jersey, including unwanted sexual messages and displays of offensive material and explained how location tracking, spyware and behaviour profiling contribute to privacy violations and abuse. Kate emphasised the need for better education and awareness among professionals to protect victims.

Legislation and Cultural Change

Kate discussed the limitations of legislation alone in addressing online abuse and the need for cultural change, highlighting the importance of viewing data privacy as a basic human right and integrating it into education and business operations. She called for addressing biases in data handling and building trust across diverse communities and described the fear of data sharing among migrant communities and its impact on accessing support services.



Kate introduced the topic of understanding and reducing inequalities in privacy rights, emphasising the importance of privacy rights being about safeguarding people, especially those most impacted by lack of protection. She shared her corporate Human Resources background and the experience of implementing GDPR in the UK in 2018 and described GDPR

Promoting Transparency and Consent

Kate pointed out the need for proactive promotion of transparency and informed consent in data collection, calling for clear, accessible privacy policies and multiple language translations to empower individuals. She advocated for internal company cultures that prioritise ethics and privacy in data handling, urging advocacy for tech companies to be held accountable for privacy impacts and collaboration across sectors to amplify voices.

Inclusive Policy Making and Education

Kate stressed the importance of involving the most vulnerable in developing solutions for data privacy, signalling for diverse representation in tech and policy development and active involvement of community leaders and activists to create a culture of self-advocacy. She recommended the need for education initiatives in schools, workplaces and communities to empower individuals and called for cultural change that values individual autonomy, promotes accountability and protects the most vulnerable from exploitation.

Key Outcomes:

- Privacy rights are about safeguarding people, especially those most impacted by lack of protection.
- Three common barriers to collecting diversity data: ignorance, fear, and trust issues. Businesses are reluctant to collate this data, together with a fear of backlash and infringing on data privacy as a significant barrier.
- There is an uneven impact of data privacy on different demographics, particularly women, children and ethnic minorities.
- Online abuse, including unwanted sexual messages and displays of offensive material, location tracking, spyware and behaviour profiling contribute to privacy violations and abuse.
- There are limitations of legislation alone in addressing online abuse and a need for cultural change, so data privacy is viewed as a basic human right.

Action Points:

- Prioritise data privacy as a basic human right and integrate this view into education policy and business operations.
- Address gender, socioeconomic and racial biases in data handling, including data privacy risks related to surveillance, harassment and misuse of sensitive information by government agencies and corporates.
- Build trust across diverse communities that corporate, government and support agencies will handle data safely and appropriately.
- Promote transparency and consent in data collection, using clear and accessible language in privacy policies, including multiple language translations.
- Evolve internal company cultures to prioritise ethics and privacy in all aspects of data handling.
- Advocate for tech companies to be held accountable for the privacy impact of their products and services.
- Involve diverse community representatives, including those who have experienced privacy violations, in developing data privacy policies and solutions.
- Educate the public, including in schools and workplaces, on data privacy rights to empower people with knowledge and self-advocacy.

SESSION 6 – INDIVIDUAL



PANEL DISCUSSION: “EDUCATION FROM THE GROUND UP: THE SOCIETAL IMPACT OF PRIVACY EDUCATION”

MODERATOR:

Patricia Kosseim, Privacy Commissioner for Ontario, Canada

PANELLISTS:

- Matthew Johnson, Director of Education, Media Smarts, Canada
- Baroness Beeban Kidron OBE, Member of the House of Lords, Founder & Chair 5Rights Foundation
- Bertrand du Marais, Commissioner for International Affairs, e-Privacy and Competition Co-regulation, CNIL
- Joyce Lai, Assistant Privacy Commissioner for Personal Data (Corporate Communications and Compliance) of the PCPD, Hong Kong
- Leanda Barrington-Leach, Executive Director, 5Rights Foundation



The session focused on the societal impact of privacy education, emphasising the need to empower children in the digital age. Key points included the UN's updated guidance on digital rights for children, the importance of integrating digital literacy into school curricula, and practical initiatives like Ontario's Youth Advisory Council and Digital Privacy Charter. Baroness Beeben Kidron highlighted the failure of adult protection mechanisms, while Joyce Lai from Hong Kong detailed their three-phase approach to privacy education. Matthew Johnson discussed the distinction between risks and hazards in digital media, and Leandra Barrington-Leach stressed the need for systemic change to protect children's privacy. A youth ambassador underscored the urgency of prioritising children's digital rights.

Patricia Kosseim introduced the session's focus on the societal impact of privacy education. She discussed the importance of digital technologies in children's lives and the need for empowerment in a digital world, referencing the UN Convention on the Rights of the Child and its updated guidance on digital environments.

Patricia spoke about the UN Committee's call for digital literacy in schools and the importance of teaching children to handle digital tools safely and responsibly. She talked about Ontario's updated curriculum to emphasise digital literacy and citizenship skills, through initiatives like the Youth Advisory Council and the Youth Ambassador Toolkit to engage youth in privacy education. Patricia also highlighted Ontario's Digital Privacy Charter for schools, which aims to empower students to understand and exercise their privacy rights. She said that recent legislative efforts in Ontario are ongoing to improve protections for children and youth, with a focus on standards that respect children's rights and values of personal autonomy.

Baroness Kidron discussed a conversation with young advisors from various countries which placed an emphasis on the collective responsibility of adults to protect children's rights and freedoms. She spoke about the importance of including children in the discussion about privacy and safety and gave a critique of the 'attention economy' and surveillance capitalism's impact on children. She highlighted the need for digital literacy and digital skills in the 21st century and the importance of systemic approaches to protect children's privacy, such as dismantling live streaming and preventing adult friend requests. She also gave examples of children using technology for positive outcomes, such as increasing farm productivity and teaching sign language, but called for privacy regulators to support companies in designing services that protect children's privacy.

Bertrand du Marais spoke about the importance of collective education and the role of privacy regulators. He also encouraged the need for an educative cartography and multi-disciplinary programs. He talked about the role of media and traditional media in raising awareness about privacy, as well as the importance of expertise and competence in addressing privacy issues.

Joyce Lai discussed the PCPD's three-phase approach to privacy education: educate, engage, and empower, with initiatives including publications, thematic websites, and interactive seminars in multiple languages. She said they address issues such as cyberbullying, doxing and AI through educational materials and competitions. Joyce talked about the importance of engaging children, parents and teachers in privacy education.

Matthew Johnson discussed the distinction between risks, hazards, and harms in the context of digital media literacy. He spoke about Media Smarts' research on youth's capacity for managing privacy and social privacy and the importance of teaching young people to recognise and manage privacy risks. Matthew advocated for a digital media literacy strategy and integrating privacy into the curriculum, stating that digital literacy gives young people a voice and that young people do care about data privacy when they understand it.

Leandra Barrington-Leach emphasised the importance of prioritising children's rights and involving them in the discussion. She talked about the role of the 5Rights Foundation in advocating for children's digital rights and providing practical support. She discussed the need for a systemic approach to protect children's privacy and empower them and the importance of consistent global standards for children's digital rights. She also emphasised the need to implement privacy by design when developing systems for young people.

Leandra introduced a video from a 13-year-old 5Rights Chief Ambassador, Skye, to offer a youth perspective on privacy and safety. Skye emphasised the importance of a safe digital environment for youth, providing a critique of companies profiting from children's data and the need for transparency. She suggested that tech companies need to prioritise privacy over profit and spoke about the importance of listening to youth and involving them in the conversation about privacy. Skye called for privacy regulators to enforce children's privacy rights and innovate for their benefit.

Key Outcomes:

- Children need to be more empowered to navigate the digital age, starting with a focus on digital literacy in schools to give them a voice.
- It is the collective responsibility of adults to protect children's rights and freedoms.
- Young people need to be involved in the conversation. Educate, engage and empower.
- Young people need to be educated to understand the distinction between risks, hazards, and harms in the context of digital media literacy so they can recognise and manage privacy risks.
- Young people want a safe digital environment and tech companies need to prioritise privacy over profit.

Action Points:

- Seek early adopters for the digital privacy charter for schools in Ontario.
- Implement the 3E strategy (Educate, Engage, Empower) for children's privacy education in Hong Kong.
- Advocate for a digital media literacy strategy at the federal and provincial levels in Canada.
- Provide practical support and tools to regulators and innovators globally to implement children's digital rights.

SESSION 6 – INDIVIDUAL



PANEL DISCUSSION: “ACCESSIBLE PRIVACY: PROTECTING THE DISABLED, VULNERABLE AND SOCIALLY MARGINALISED IN A DIGITISED WORLD”

MODERATOR:

Alex White, Commissioner, Bermuda

PANELLISTS:

- John Edwards, Information Commissioner, UK ICO
- Philippe Dufresne, Commissioner, Office of the Privacy Commissioner, Canada
- Beatriz Anchorena, Director, AAIP Argentina
- Carly Kind, Privacy Commissioner, Office of the Australian Information Commissioner

The panel discussed accessible privacy, focusing on vulnerable groups like domestic abuse victims, indigenous communities and those with mental health issues. Carly highlighted large data breaches in Australia, affecting over 14 million people. John emphasised identifying unmet needs, citing a project on migrant tracking. Beatrice discussed Argentina's efforts to bridge digital gaps, particularly for children and the disabled. Philippe stressed the importance of privacy by design and accessibility, noting widespread issues with dark patterns. The panellists agreed on the need for empathetic, user-friendly approaches and systemic changes to protect vulnerable populations.

Alex White introduced the panel and its purpose, which is to discuss accessible privacy for individuals with disabilities, vulnerabilities or social marginalisation. He emphasised the dual nature of technology: it can enable but also pose risks to these individuals. Alex explained that the session aimed to explore how technology and data can be used to help without causing additional harm.

Carly Kind provided an overview of large data breaches in Australia, including the MediSecure breach affecting 14 million Australians. She explained that the breaches have led to personal information being made public, exacerbating harm to

vulnerable groups. She highlighted three groups particularly affected: domestic abuse victims, indigenous communities (Eg device sharing – consensual and non-consensual), and people with mental health problems. She said that indigenous



communities face unique challenges, such as device sharing and concerns about cultural knowledge loss. She also talked about mental health patients who are often adversely affected by the emotional impact of data breaches, leading to exemptions from notification to avoid additional trauma. Carly discussed the complexities of government data use, particularly in the context of veterans' data being used for mental health research. She talked about The Department of Veteran Affairs' program which was found to undermine mental health due to a lack of robust consent.

John Edwards shared insights from his experience as a Data Protection Authority in New Zealand and the UK, focusing on identifying unserved communities. He described a pilot project on geo-locating ankle tags for migrants, which was discontinued due to its corrosive effect on their sense of security and well-being. John spoke about how victims of serious sexual violence (mainly women) are often re-victimised by investigative techniques, leading to a call for better support. Eg. Digital strip searches, having devices taken, access to medical and counselling records etc. He said women felt they were the ones being investigated. He talked about traveller communities and children as other groups identified as having unmet needs in data protection. He explained it is hard to find the groups we're not reaching and that the UK ICO have prioritised children, who are often unaware of their rights. John explained how men living with HIV were found to be abandoned by controllers after data breaches, prompting a campaign to raise awareness of the human impact of breaches, such as the marginalisation of men who had been exposed by data breaches. He suggested there should be more focus on the data subject, not just the controller and emphasised the need for empathetic and accessible communication in data protection efforts.

John talked about the 'ripple effect' of data breaches, suggesting we separate the incident from the impact of the breach. He said that controllers have a duty to the people that have been affected. He said that vulnerability is not a mark on people. Rather, it's contextual, with 70% of people who have experienced a breach suffering some sort of negative impact, such as loss of employment, loss of empowerment, insecurity and fear. He said that 25% said they had no support from the organisation that caused the breach. John mentioned that the UK ICO call centre staff are now all trained in trauma response and encouraged controllers to remember the real-world impact and that there's a person at the end of their actions.

Beatriz Anchorena discussed the digital and educational gaps in Argentina, particularly among children and teenagers. She said the COVID-19 pandemic highlighted the lack of access to computers and internet, with 42% of households lacking these resources in October 2021. She commented that the paradox is that it allows greater access to information and resources, but it also comes with risks and challenges. Beatriz said that Argentina's Data Protection Authority had developed educational guides for children and teenagers on privacy and data protection, working with 23 provinces to provide training and awareness-raising activities on privacy rights. She highlighted the importance of consent, age assurance, and privacy policies for vulnerable populations, including children and disabled individuals.

Philippe Dufresne emphasised the coexistence of privacy and accessibility, noting that privacy supports other human rights. He talked about privacy by design and accessibility by design, suggesting they are not in conflict but build on each other, aligning with the Convention on the Rights of Persons with Disabilities. Philippe shared experiences with accessibility cases, including the need for dignified communication and support. How do we communicate to the outside world, including these vulnerable groups? He talked about a privacy sweep on dark patterns (hard to understand or read) that revealed widespread issues, particularly on websites designed for children (see OPC Canada's report). He called for better design practices to make choices easy to understand and remove barriers for all users, including children and persons with disabilities.

Alex asked panellists for practical steps that can be taken in their offices to improve privacy practices. John suggested focusing on individual needs and providing a customer service approach tailored to each person's experience, putting the individual at the forefront. Beatriz recommended mapping vulnerable populations and developing specific plans for each group and skills to address their needs. Carly questioned the balance of regulatory tools and their proportionate use across issues and groups. What is the right way to use our tools in a proportionate manner? Vulnerability is a key factor in deciding which cases to investigate. Philippe emphasised the importance of incentivising good behaviours and making communications user-friendly for both industry and individuals.

Key Outcomes:

- Technology has a dual nature: it can enable but also pose risks to individuals.
- Domestic abuse victims, indigenous communities and people with mental health problems are particularly affected.
- Victims of serious sexual violence (mainly women) are often re-victimised by investigative techniques and need better support.
- Some communities, such as traveller communities, children, marginalisation of men who had been exposed by data breaches, identified as having unmet needs in data protection and are abandoned by controllers after data breaches. There is a need to raise awareness of the human impact of breaches.
- 70% of people who have experienced a breach suffer some sort of negative impact, such as loss of employment, loss of empowerment, insecurity and fear. 25% had no support from the organisation that caused the breach.
- There is a coexistence of privacy and accessibility, noting that privacy supports other human rights.

Action Points:

- Conduct a mapping of vulnerable populations (children, disabled, social security) and develop specialised instruments and skills for the agency to respond to their needs.
- Challenge people within the organisation to make communications and guidance more user-friendly, both for industry and individuals, particularly for children.
- Develop better design practices to make choices easy to understand and remove barriers for all users, including children and persons with disabilities.
- Review the age assurance code and consider signing up for it.

SESSION 7 – INTEGRITY



PANEL DISCUSSION: “CREATING TRUST THROUGH DATA TRUSTS”

MODERATOR:

Rachel Harker, Digital Jersey

PANELLISTS:

- Dame Wendy Hall, University of Southampton
- Jack Hardinges, Foresight
- Carolyn Lang, Pinsent Masons

The discussion focused on the concept of Data Trusts, emphasising their role in multi-party data sharing for public benefit. Rachel Harker introduced the Jersey Data Trust, highlighting its success in collecting over 100,000 kilometres of cycling data from 500 cyclists, which informed road safety improvements. Dame Wendy Hall and Jack Hardinges discussed the broader implications of Data Trusts, including their potential in AI and health data sharing. Carolyn Lang addressed legal and governance challenges, stressing the need for clear purposes and value propositions. The panel agreed on the importance of trust, transparency, and responsible data governance to promote public trust in data sharing initiatives.

of data trusts in governing data and building confidence in data usage. Rachel described Jersey's unique trust laws and the establishment of the Jersey Data Trust, and explained the challenges faced by Digital Jersey in data sharing and the creation of the Jersey Data Trust. She detailed the Jersey Data Trust's purpose, structure, and administration by an independent trustee, before discussing the success of the Jersey Data Trust in collecting cycling data and its impact on road safety and infrastructure. Rachel then announced the next phase of the Jersey Data Trust: the Jersey Data Exchange, explaining the expansion of data trust services to other industries, including built environment, smart cities, and health.

Dame Wendy began her introduction, emphasising the importance of data quality for AI and the challenges of implementing data trusts in the UK. She discussed the origins of the data trust concept and its relevance to AI and data quality. She stated that any country that doesn't grasp and embrace AI is lost. But you can't do AI without a data strategy. She highlighted the complexities of implementing data trusts in the UK, particularly in the health sector, but praised Jersey's unique trust laws and the potential for Jersey to lead in data trust innovation. To conclude, Dame Wendy emphasised the importance of adapting trust laws for data trusts and the potential for Jersey to export this model globally.

Jack Hardinges introduces his background and experience with data sharing institutions. He discussed his work with Foresight and the recruitment of half a million people for eye scans for medical research, then explained the emerging field of oculomics and its potential for early disease detection. Jack highlighted the challenges and opportunities in balancing data access and commercial value in health research.

Carolyn Lang introduces her role at Pinsent Masons and her work on data privacy, data licensing, and data strategy. She spoke about her involvement in the UK water sector collaboration to make data open for innovation and mentioned her work on the UK's digital twin project and the challenges of standardising data sharing agreements. Carolyn emphasised the importance of governance and legal structures in successful data sharing initiatives.

Rachel asked the panellists about the opportunities and barriers in data sharing. Dame Wendy suggested the importance of foundations and governance in digital twins and personal data stores, while Jack discussed the potential of oculomics and the challenges of valuing data access. Carolyn highlighted the importance of clear purpose, value proposition, and governance in data sharing initiatives.

Dame Wendy discussed the challenges of global data sharing and the need for legal vehicles to enable it. Jack emphasised the importance of trust and good governance in data sharing, and Carolyn mentioned the need for compliance and transparency to build trust in data sharing projects.



Rachel Harker introduced the panel, discussing data trusts and multi-party data sharing for public good. She explained the concept of data trusts, referencing Dame Wendy's 2017 UK Government AI review, and highlighted the importance

Key Outcomes:

- Data trusts will be important in governing data and building confidence in data usage.
- Data quality is essential for AI and the challenges of implementing data trusts in the UK.
- Jersey's unique trust laws created the potential for Jersey to lead in data trust innovation, but amendments to local Trust Law will be needed.
- There are challenges and opportunities in balancing data access and commercial value in health research.
- There needs to be a clear purpose, value proposition, and governance in data sharing initiatives.

Action Points:

- Explore the potential of data trusts and data sharing structures in other sectors beyond cycling, such as the built environment, smart cities, and healthcare.
- Develop methods to better assess and compare data governance practices across different data infrastructures and initiatives.
- Ensure compliance with data protection regulations is seen as an enabler rather than a barrier and use it to build trust in data sharing projects.
- Educate the public on the value of personal data management and the benefits of well-governed data sharing frameworks.

SESSION 7 – INTEGRITY



PANEL DISCUSSION: “TRUST AND SAFETY FOR AUTOMOBILE INNOVATION”

MODERATOR:

Dan Caprio, Providence Group, Vice Chair,
US Department of Commerce IoT Advisory Board

PANELLISTS:

- Maarten Botterman, Former ICANN Chair, IGF IoT Dynamic Coalition Chair, Amsterdam
- Jonathan Cave, University of Warwick
- Andreea Lisievici Nevin, Privacy Digital & AI Consultant.

The panel discussed the governance challenges and opportunities surrounding connected cars, emphasising the need for transparency, accountability, and privacy. Dan Caprio highlighted the US Department of Commerce's recommendation for labelling connected cars to inform consumers about data use. Maarten Botterman stressed the importance of ethical data practices and meaningful transparency. Andrea Nevin noted the complexity of data collection and processing in cars, advocating for early transparency and accountability. Jonathan Cave underscored the need for data to serve people and warned against over-reliance on data, suggesting live and smart labels for ongoing updates. The panel agreed on the necessity of a cultural shift towards responsible data use and governance.

Dan Caprio started the session by introducing the report released last week by the US Department of Commerce's Internet of Things Advisory Report, which recommends creating a label for connected cars to inform consumers about data usage. He outlined the governance challenge posed by connected cars, emphasising the need for transparency and honesty in data practices. Dan referenced the Texas case against General Motors, where GM used technology to collect and sell detailed driving data without informing customers, who then sold that data to two companies to generate scores on the drivers and sold it insurance companies. He stressed the importance of good corporate governance, including assessing data risk, being honest with consumers, and ensuring transparency in data practices.

Maarten Botterman provided his perspective on governance and the challenges faced by connected cars. He discussed the importance of using data responsibly and ethically, emphasising the need for transparency and informed consent. He also shared his experience with connected devices, such as his Samsung TV, which sent voice data to Korea for improvement without considering privacy. Maarten highlighted the development of IoT good practice principles to ensure ethical and sustainable use of IoT systems from the outset of development and called for a balance between adequate privacy and public interest, emphasising the need for meaningful transparency and user control over data.



Andreea Nevin expanded the discussion to include proportionality and accountability, particularly in the context of risk-based legislation like the GDPR. She explained the challenges faced by car manufacturers in complying with privacy requirements, which are often compliance-based rather than risk-based. She discussed the broader ecosystem of stakeholders involved in car data processing, including third parties and physical components in the car. Andrea emphasised the need for early transparency about data processing and the importance of privacy labels on cars to inform consumers.

Jonathan Cave discussed the role of governance in ensuring that data serves people and the importance of trust in the relationship between consumers and corporations. He highlighted the need for clear and understandable information about data collection and use, particularly at the point of purchase, emphasising the importance of considering the long-term consequences of data collection and use, including the potential for unintended consequences. Jonathan called for a cultural shift towards responsible data use and the need for regulators to ensure that data practices align with public interest.

Dan Caprio reiterated the importance of data serving people and the need for a cultural shift towards responsible data practices and emphasised the need for a multi-stakeholder approach to governance, including CEOs and Boards driving a culture where data serves people. Maarten called for a cultural change and the need for responsible data practices to avoid the pitfalls seen in other industries, while Jonathan highlighted the importance of framing data governance issues in a positive light to encourage cooperation and innovation and repeated that data should serve people, not replace them. He finished by suggesting that we should have live, smart labels, rather than labels that go out of date the moment they leave the showroom.

Key Outcomes:

- Transparency and honesty in data practices is required to address the governance challenge posed by connected cars.
- The development of IoT good practice principles is needed to ensure ethical and sustainable use of IoT systems from the outset of development and strike a balance between adequate privacy and public interest.

- Car manufacturers face challenges with complying with privacy requirements, which are often compliance-based rather than risk-based.
- Early transparency about data processing and of privacy labels on cars to inform consumers would reduce risk.
- Data should serve people, not replace them.
- Car manufacturers need to consider the long-term consequences of data collection and use, including the potential for unintended consequences.
- There needs to be a cultural shift towards responsible data use and the need for regulators to ensure that data practices align with public interest.

Action Points:

- Establish a multi-stakeholder connected car working group under the Global Privacy Assembly to study and recommend global best practices and standards for connected cars.
- Ensure that data collected from connected cars primarily serves the interests of the people using the cars, not just the interests of the car manufacturers or other entities.
- Consider whether a certain connected feature is truly necessary and proportionate to the user's needs before implementing it in a car.
- Explore the use of "live and smart" labels for connected cars to provide up-to-date information to consumers about data practices, as the technology and data uses may change over time.
- Encourage a cultural shift towards responsible and accountable data practices in the car industry, guided by recommendations and standards, to ensure that connected car technology does not "derail" into unintended and harmful directions.



SESSION 8 – INFORMATION



PODIUM DEBATE: “DATA MINIMISATION: A TRUE GUIDANCE POINT, OR A RELIC?”

MODERATOR:

Jules Polonetsky

RED CORNER:

Philippe Dufresne, Privacy Commissioner of Canada

BLUE CORNER:

Sheila Colclasure, Global Chief Digital Responsibility and Public Policy Officer @ IPG/Kinesso



The debate focused on the topic of data minimisation versus the need for data to drive innovation, competition, and equity. Philippe Dufresne, Privacy Commissioner of Canada, emphasised the necessity of data minimisation for privacy, innovation, and trust, citing historical and contemporary examples. Sheila Colclasure from IPG argued for a more flexible approach, highlighting the incompatibility of strict data minimisation with innovation, competition, and equity. She stressed the need for a context-specific, proportional approach to data collection. Both agreed on the importance of context and proportionality in data governance, aiming to balance privacy with innovation and competition.

Opening Remarks and Introduction to the Debate

Jules Polonetsky introduced the debate format, emphasising the importance of testing and challenging ideas to foster learning. He outlined the purpose of the event and the role of debates in engaging with complex data protection issues. He spoke about the debate structure, featuring Philippe Dufresne, Privacy

Commissioner of Canada, arguing in favour of data minimisation, and Sheila Colclasure IPG, questioning whether data minimisation was hindering business progress and innovation. The format included seven-minute opening statements, rebuttals, and audience engagement to decide the winner.

Philippe Dufresne’s Argument for Data Minimisation

Philippe highlighted the importance of privacy principles in protecting individual freedoms and preventing historical abuses like surveillance states. He emphasised the relevance of Canadian privacy legislation, which is based on fair information principles and is technologically neutral, and therefore future-proofed. Philippe argued that data minimisation is a core principle that supports innovation, competition, and trust in the economy and public institutions. He referenced historical and contemporary examples to illustrate the need for privacy protections, privacy as a fundamental human right, and the dangers of unconscious bias and over-collection of personal data.

Sheila Colclasure’s Counterargument on Data Maximisation

Sheila Colclasure argued that strict data minimisation principles are incompatible with innovation, competition, equity, and practicality. She highlighted the need for a more flexible approach to data collection that allows for innovation and competition, especially for small businesses. Sheila pointed out that many small businesses lack access to necessary data, which hinders their ability to compete effectively. She emphasised the importance of data in creating equity and fairness, arguing that strict minimisation can lead to unfair biases and discrimination.

Rebuttal and Final Arguments

Philippe responded to Sheila’s arguments, emphasising the importance of minimising personal data while allowing for the use of non-personal data. He argued that innovation and competition can coexist with privacy protections, citing examples of privacy-enhancing technologies and collaborations with competition authorities. He highlighted the risks of over-collection, including the potential for data breaches and government overreach.

Sheila reiterated the need for a more contextual and flexible interpretation of data minimisation, arguing that strict application is impractical and detrimental to innovation and competition.

Audience Interaction and Closing Remarks

The audience was given an opportunity to provide quick interjections, with one speaker emphasising the cost-saving benefits of data minimisation and reducing the attack surface. Another speaker asked whether a reasonable amount of data collection, rather than strict minimisation, would be a more appropriate approach. Both debaters agreed that context and proportionality are essential in interpreting data minimisation principles.

Jules Polonetsky concluded the debate, thanking the participants and presenting them with challenge coins, symbolising the ongoing importance of the privacy debate.

Key Outcomes:

- Privacy principles protect individual freedoms and prevent historical abuses like surveillance states.
- Data minimisation is a core principle that supports innovation, competition, and trust in the economy and public institutions. Innovation and competition can coexist with privacy protections
- Or it could be argued that strict data minimisation principles are incompatible with innovation, competition, equity, and practicality.
- There is a need for a more flexible approach to data collection that allows for innovation and competition, especially for small businesses and can lead to unfair biases and discrimination.
- Either way, context and proportionality are essential in interpreting data minimisation principles.

Action Points:

- Work together as data protection authorities, industry, and other stakeholders to find solutions that reconcile privacy protection with innovation and competition.
- Innovate and create a more flexible, interpreted approach to data minimisation that allows for innovation, competition, and equity while still protecting privacy.
- Consider the principle of proportionality when interpreting data minimisation requirements, finding a reasonable amount of data collection rather than strict minimisation or unlimited collection.

SESSION 8 – INFORMATION



FIRESIDE CHAT: “COPING WITH THE EXTREME”

MARTINE WRIGHT MBE (INTERVIEWED BY JESS DUNSDON, ITV JERSEY)

Martine Wright, an MBE recipient and Paralympian, shared her inspiring journey post-2005 London bombings, where she lost both legs. Despite the trauma, she found purpose in competing in sitting volleyball at the Paralympics and became a mother. She highlighted the challenges of privacy and data protection post-accident, including unauthorised media use and bureaucratic hurdles in claiming benefits. Wright criticized the government's compensation scheme for not adequately valuing multiple disabilities and emphasised the need for accurate information and understanding of disabilities. She advocated for better support systems and the importance of using one's voice to fight for rights.

Introduction

Jess Dunsdon welcomed Martine Wright, MBE, to discuss her inspiring story. Martine lost both her legs in the London 7/7 tube bombings 19 years ago and was the last survivor pulled from the wreckage. Since then, she has shown remarkable resilience, achieving significant milestones such as captaining Team GB at the Paralympics in sitting volleyball, learning to fly, and becoming a mother. She has also received numerous awards, including an MBE, and has become a celebrated sports presenter.

Martine's Experience on 7/7

On July 7, 2005, Martine was a passenger on the London Underground when she sat next to a suicide bomber. She recalled a moment of confusion followed by devastation, with no memory of pain, only the sight of metal and the smell of burning. A police officer, Liz Kenworthy, played a crucial role in saving her life. Martine emphasised her luck in surviving and the importance of her journey since that day.





Turning Point and Mindset

Initially, Martine said she struggled with the question “Why me?” during her recovery. However, after two months in the hospital, she realised she had a choice: to feel sorry for herself or to embrace life. She found inspiration in meeting other victims and recognised that many had faced worse circumstances. This realisation motivated her to pursue her dreams, including participating in the Paralympics.

Press Intrusion and Privacy Issues

Martine explained how she experienced significant press intrusion during her recovery, which was her first encounter with privacy violations. Despite her background in data protection, she found herself overwhelmed by the number of people involved in her care and the media’s interest in her story. She was shocked to discover that a magazine published a photo of her without permission, highlighting the lack of respect for her privacy during a vulnerable time.

Government Bureaucracy and Disability Benefits

Martine also faced challenges navigating government bureaucracy while applying for disability benefits. She recalled how she had to fill out forms based on her worst days, which was emotionally taxing, and resulted in her providing more sensitive personal information than normal. After transitioning from Disability Living Allowance to Personal Independence Payment (PIP), she was denied benefits despite her disabilities. This experience underscored the flaws in the system, where her visible disabilities were not adequately recognised.

Compensation Scheme Issues

Martine explained how the government compensation scheme penalises individuals with multiple disabilities, offering lower compensation for additional injuries. It again highlighted how disabled people are forced to provide more information than necessary as a result of their disability. Martine expressed her frustration with the outdated system, which fails to account for the true value of lost limbs and the psychological impact of such injuries. She has advocated for change, emphasising the need for a more compassionate and accurate approach to compensation.

Classification in the Paralympics

Martine described how in the Paralympics, athletes must undergo a classification process that can feel like a fight to prove their disabilities, again providing more information than an able-bodied athlete. She noted that this is the only time disabled individuals are encouraged to present themselves as more disabled than they are. The classification system can be strict and sometimes unfair, as it often relies on individuals who may not fully understand the nuances of different disabilities.

Responsibility and Advocacy

Martine said she felt a strong sense of responsibility to advocate for others who may not have the strength to fight for their rights. She views her achievements, including receiving her MBE and participating in the Paralympics, as a way to honour her family and friends who supported her. She believes in using her voice to raise awareness and push for change in how society treats individuals with disabilities.

Call for Change

Martine emphasised the need for accurate information and representation in media, government, and organisations. She advocated for involving disabled individuals in decision-making processes to ensure their experiences and needs are understood. Martine believes that by working together, society can create a more inclusive and supportive environment for everyone.

Conclusion

In closing, Martine Wright’s story is one of resilience, advocacy, and the pursuit of a better future for individuals with disabilities. Her experiences highlight the importance of understanding, compassion, and the need for systemic change in how society addresses disability and privacy issues.

Key Outcomes:

- Victims of terrorism were exposed to a lack of respect for her privacy during a vulnerable time.
- There are distinct differences in how disabled people are treated in terms of their privacy in comparison to able-bodied people.
- Understanding, compassion, and the need for systemic change in how society addresses disability and privacy issues.

Action Points:

- Advocate for changes to the government compensation scheme for victims of terrorist attacks to make it fairer and more equitable.
- Encourage the government, media, and regulators to involve more people with disabilities in policy decisions and processes that impact the disabled community.
- Continue to engage with advocates for vulnerable people to provide a voice and fight for the rights and needs of people with disabilities who may not have the strength or ability to advocate for themselves.

GALA DINNER AND AWARDS CEREMONY

As much a part of the conference content is the opportunity to network and engage with experts in a more social setting. This year, the organisers wanted to maximise the opportunity by hosting a gala dinner for delegates, including the annual GPA Awards which, now in its eighth year, celebrate the achievements of the GPA community and shine a light on good practice.

The awards are open for any GPA Member Authority to enter, and entrants provide a detailed description of their initiative, along with their explanation as to why they think it deserves an award.

THERE ARE 5 MAIN CATEGORIES, NAMELY:

- Education and public awareness
- Innovation
- Accountability
- Dispute Resolution & Enforcement
- People's Choice

Entries can relate to any initiative taken by the member authority since January 2022, until the entry closing date. Initiatives can include anything at all, such as any guidance resource, investigation, tool, publication, video, conference, website, partnership, poster, speech, policy, app, intervention, etc.

This year there were 61 entries into all categories, making it a significant challenge for the Executive Committee when it came to shortlisting. In addition to those 5 categories, the hosts also presented the Giovanni Buttarelli Award, in memory of a dear friend and respected colleague.

The awards presented are detailed as follows:



CATEGORY A: EDUCATION AND PUBLIC AWARENESS

There were a staggering 37 entries to this category. This category is largely influenced, albeit not exclusively by the valuable work in the GPA Digital Education Working Group (DEWG). The DEWG has created tools for authorities to make their efforts in digital education available to peers and helped instil a culture of sharing experience in that space. Other public awareness initiatives were also considered, including those that are not in the digital space.



**WINNER: CATALAN DATA PROTECTION AGENCY FOR THEIR PROGRAM
“WHO ARE YOU? DATA THAT SPEAKS ABOUT YOU”.**

CATEGORY B: INNOVATION

There were 12 entries for this category. Entrants are required to set out how an initiative/project undertaken is working effectively to support innovation and address disruptive business models. The award helps to illustrate how GPA members are using innovation to deliver their own work more effectively.



**WINNER: SPANISH DATA PROTECTION AGENCY (AEPD) FOR THEIR INITIATIVE DESIGNED TO
SHOW THEIR COMMITMENT TO CHILDREN'S PROTECTION, ALIGNING DATA PROTECTION
RIGHTS AND EVIDENCE-BASED INNOVATION TO IMPROVE ONLINE SAFETY STANDARDS.**

CATEGORY C: ACCOUNTABILITY

There were 8 entries to this category. Even when not explicit in the law, the accountability of organisations processing personal information is implicit in most privacy and data protection laws. This category asks what member authorities are doing to promote this concept of accountability and ensure that it makes the successful transition from law to practice.



WINNER: AGENCY FOR ACCESS TO PUBLIC INFORMATION (AAIP) ARGENTINA FOR THEIR PERSONAL DATA PROTECTION MODULE, WHICH IS THE FIRST FREE OF CHARGE ONLINE TOOL FOR PERSONAL DATA PROTECTION COMPLIANCE IN ARGENTINA, GUIDING DATA CONTROLLERS AND DATA PROCESSORS ON THE PRINCIPLE OF ACCOUNTABILITY.

CATEGORY D: DISPUTE RESOLUTION & ENFORCEMENT

There were 4 entries to this category. This category builds upon the focus that the Conference has placed on enforcement cooperation in several resolutions in recent years. It reflects the multi-faceted roles that Data Protection and Privacy Authorities perform which always covers at least one of the following roles and often encompass both:

- Dispute resolution: mediating or investigating and resolving issues where it appears to an individual that the law has been breached.
- Enforcement: taking many forms, enforcement involves taking formal action in relation to non-compliance with the law.



WINNER: UK INFORMATION COMMISSIONER'S OFFICE (ICO) FOR THEIR INITIATIVE TO IMPROVE DESIGN PRACTICES IN DIGITAL MARKETS IN CONJUNCTION WITH THE UK COMPETITION AND MARKETS AUTHORITY, ALONG WITH THEIR REGULATORY ACTIVITY TO IMPROVE THE COOKIE BANNER DESIGN PRACTICES OF MANY OF THE UK'S TOP WEBSITES.

PEOPLE'S CHOICE AWARD:

The People's Choice Award features once again in this year's award line-up and was subject to an open vote among GPA members from amongst all shortlisted candidates of each of the other awards' categories.

WINNER: SPANISH DATA PROTECTION AGENCY (AEPD)



GIOVANNI BUTTARELLI AWARD

The Giovanni Buttarelli Award is a distinguished honour, dedicated to the memory of a much-loved and remembered colleague, former European Data Protection Supervisor and esteemed Host of the GPA conference 2018 in Brussels. The Award symbolises the GPA's commitment to fostering leadership on an international scale and promoting collaboration across boundaries.

All GPA Members can nominate one or more candidates, with whom they have closely collaborated, belonging to an organisation in the field of data protection or privacy.

Once again this year, the field of shortlisted candidates was very strong indeed, again demonstrating the high calibre of expert professionals working in the field of privacy and data protection.

WINNER: MR BRUNO GENCARELLI

Now as Expert Member to the Cabinet of Justice Commissioner, Bruno Gencarelli has been at the forefront of data protection law for nearly 15 years. He has headed up the International Relations Sector on data protection, been deputy head of unit and then head of unit for data protection, head of unit for International data flows and protection, Deputy Director for Fundamental Rights & the Rule of Law, and Head of the International Affairs and Data Flows Unit before taking up his current position in June 2024.

Part of his work included a leading role in the EU-US negotiations on transatlantic data flows in both the commercial and law enforcement areas. This included leading the Commission's delegation in the inter-institutional negotiations with the European Parliament and the Council on the data protection reform (now better known as the GDPR and "Law Enforcement Directive").

Bruno also led the negotiations on the EU-Japan mutual adequacy arrangement creating the world's largest area of free and safe data flows. He recently co-led for the EU the negotiations with the UK on all aspects relating to justice and consumers in the context of Brexit and was in charge of the adequacy process with respect to the UK and the negotiations with the US on a successor arrangement to the PrivacyShield.

Bruno previously served as a member of the European Commission's Legal Service and as an assistant (Référéndaire) to a judge at the European Court of Justice after having practiced law in the private sector. He holds degrees in law and political science and is an author of numerous publications on EU law.



With the formal part of the evening concluded, the organisers were keen to celebrate the successes of all delegates in terms of their contribution to privacy and data protection. Following a surprise presentation to retiring Jersey Data Protection Authority Chair, Jacob Kohnstamm, the delegates were entertained with live music and dancing, courtesy of Jersey Information Commissioner, Paul Vane's band, Inside Job.



DAY 4: THURSDAY 31ST OCTOBER 2024

Closed Session for GPA Members only.

DAY 5: FRIDAY 1ST NOVEMBER 2024

Closed Session for GPA Members only.

RESOLUTIONS ADOPTED AT THE CLOSED SESSION

Resolution on surveillance and protecting individuals' rights to privacy

This Resolution builds on a number of previous Resolutions: Privacy by Design (2010), Big Data (2014), Surveillance and Law Enforcement Access to Data (2016), Ethics and Data Protection in AI (2018), Government Access to Data, Privacy and the Rule of Law: Principles for Government Access to Personal Data Held by the Private Sector for National Security and Public Safety Purposes (2021), and the Resolution on Principles and Expectations for the Appropriate Use of Personal Information in Facial Recognition Technology (2022).

The purpose of this Resolution is to emphasise the importance of comprehensively assessing necessity and proportionality of data collection through surveillance, and ensuring the concept of data minimisation is applied to the purposes being pursued. It also requires robust security measures to be undertaken by organisations adopting surveillance practices and seeks collaboration between the GPA, Data Protection Authorities and organisations to develop common standards, policies and guidelines to ensure the ethical and responsible use of surveillance technologies.

Resolution Endorsing and Encouraging the Use of Data Protection Certification Mechanisms

This Resolution seeks to create greater efficiencies in GPA actions and recalls the challenges of jurisdictional limitations created by privacy and data protection laws globally in terms of effective recourse for individuals. More specifically, the Resolution calls for the endorsement of a general principle for the use of approved privacy and data protection certification mechanisms to enable organisations to demonstrate compliance with respective laws and facilitate easier cross-border data transfer arrangements.

Resolution on principles regarding the processing of personal information in neuroscience and neurotechnology

This Resolution takes note of the rapid and significant advances in neurotechnologies, neuroscience, and neurodata collection. It seeks to address the privacy concerns arising from the use of such data and to ensure that scientific progress in neuroscience and neurotechnology is conducted in a manner that respects and protects the rights and interests of individuals. The Resolution resolves to establish comprehensive principles for the ethical and lawful processing of personal information within the domain of neuroscience and neurotechnology. The principles apply to all individuals, organisations, and entities engaged in the collection, processing, or utilisation of neurodata and related personal data, adhering to sectoral and ethics applicable standards.

Resolution on Data Free Flow with Trust and an effective regulation of global data flows

This Resolution recognises that jurisdictions around the world have been developing data protection laws that share a number of commonalities with respect to substantive requirements as well as independent oversight and effective redress. It also recognises the need for international efforts to continue to build upon these commonalities, complementarities and elements of convergence in order to foster future interoperability between them. It recalls the Resolution on "Achieving global data protection standards: Principles to ensure high levels of data protection and privacy worldwide" (2023), and calls on global regulators, law and policymakers to foster convergence on high standards and future interoperability when developing or updating data transfer tools, and commit to support efforts to bridge the differences in regulatory systems to ensure greater interoperability.

Resolution on the GPA Rules & Procedures

The purpose of this Resolution was to incorporate proposed changes to rules and procedures of the GPA, which aim to foster a Secretariat that is both flexible and robust, thereby enabling the Assembly to delineate the Chair's role separately from that of the Secretariat. Furthermore, it seeks to enhance the delineation of responsibilities between the Secretariat, the Chair, and the Executive Committee, thus fostering improved management practices and heightened coordination of pertinent activities. The Resolution also looks to adopt electronic voting for the approval of Resolutions within the GPA rules and procedures in order to help modernise and streamline the process for GPA decision making.

SIDE EVENTS

Throughout the week, a full programme of side events took place utilising multiple venues outside of the main conference programme:

Monday 28th October:

- GPA International Enforcement Working Group
Rocco 1 & 2, Radisson Blu Hotel, St Helier
- Mandat International: 'International Data Protection Certification: Convergence and Interoperability'
Golden Apple Suite, Pomme d'Or Hotel, St Helier
- Meeting of the Association Francophone des Autorités de Protection des Données Personnelles (AFAPDP)
Rocco 3, Radisson Blu Hotel, St Helier
- GSMA Roundtable: Smart Data Privacy Implementation
Le Hocq Suite, Radisson Blu Hotel, St Helier

Tuesday 29th October:

- Centre for Information Policy & Leadership Dinner
'Outcomes-Based Regulation & Cooperation'
Grand Suite, Grand Hotel, St Helier

Wednesday 30th October:

- Meta Panel Discussion: 'Working Together for Success in AI Governance'
Celestial Hall, Royal Yacht Hotel, St Helier
- UK ICO: Children's Privacy
Le Hocq Suite, Radisson Blu Hotel, St Helier
- Centre for Information Policy & Leadership
'The Silver Lining: Cloud Computing as a Building Block for Digital Transformation and AI'
Noirmont Suite, Radisson Blu Hotel, St Helier
- Microsoft Sponsor's lunch
Banjo, St Helier
- Future of Privacy Forum side event
La Mare Wine Estate, St Mary
- OPC Canada side event
'Enforcement Trilogy'
Golden Apple Suite, Pomme d'Or Hotel, St Helier
- European Commission side event
'The OECD Declaration on Government Access to Data'
Leopold Suite, Grand Hotel, St Helier

Thursday 31st October:

- Adequate Countries Meeting
Le Hocq Suite, Radisson Blu Hotel, St Helier
- GPA Digital Education Working Group Meeting
Golden Apple Suite, Pomme D'r Hotel, St Helier



COMMON OUTCOMES ARISING ACROSS ALL PILLARS

1. A COMPLEX REGULATORY ENVIRONMENT

An increase in legal instruments across the global legislative framework is causing difficulties:

- o Cross-regulatory tensions;
- o Barriers to innovation;
- o A complex regulatory environment;
- o Existing regulatory mechanisms are struggling to keep up with the challenges posed by emerging technologies;
- o Businesses are struggling to navigate the complexity of managing multiple overlapping regulatory demands;
- o There is a diversity of privacy standards, complexity in application and a need for cohesion in digital policy issues.

2. COLLABORATION IS KEY

Across a number of the theme's pillars, collaboration was mentioned as a key component to success:

- o Collaboration with data protection authorities, privacy commissioners, and other humanitarian organisations helps to develop meaningful applications of data protection principles;
- o Collaboration with other DPAs and technology processors is critical for future success;
- o Capacity issues amongst DPAs means that collaboration with NGOs is essential;
- o There is a need for collaboration between privacy and safety teams within companies to address both privacy and online safety harms;
- o Collaboration with data protection authorities, privacy commissioners, and other humanitarian organisations helps to develop meaningful applications of data protection principles;
- o Diverse legislation leads to fragmented information in Europe, due to different ideologies of medical health.

3. WE NEED TO DO MORE INVOLVING YOUNG PEOPLE.

Future prosperity is dependent upon laying the right foundations with our younger generations and involving them in the journey:

- o Young people see privacy as a basic right but have difficulty controlling what is shared online;
- o Young people often underestimate the amount of information they post online and must be mindful of the negative impact of social media on mental health, attention spans, sleep and social relationships;
- o Anonymity provided by online platforms can encourage bullying behaviour;
- o There is still a lack of focus on education around digital rights and privacy amongst children;
- o Children need to be more empowered to navigate the digital age, starting with a focus on digital literacy in schools to give them a voice;
- o It is the collective responsibility of adults to protect children's rights and freedoms;
- o Young people need to be involved in the conversation. Educate, engage, and empower;
- o Young people need to be educated to understand the distinction between risks, hazards, and harms in the context of digital media literacy so they can recognise and manage privacy risks;
- o Young people want a safe digital environment and tech companies need to prioritise privacy over profit.



4. WE MUST NOT FORGET ABOUT THE IMPACT ON HUMANITY OR HOW TO ADDRESS REAL HARMS.

Privacy harms are challenging to unpack. The individual must remain at the heart of everything we do:

- o There is a trend of human systems becoming more complex over time, leading to a contraction of human freedom;
- o The global impact of cultural innovations and their ripple effects on human flourishing;
- o A holistic approach with systematic and consistent measurement is needed when defining privacy harms. Harm is difficult to prove;
- o Demonstrating harm is challenging. It is important to address manipulation in data processing, and discussions must include those who are being impacted;
- o Online abuse, including unwanted sexual messages and displays of offensive material, location tracking, spyware, and behaviour profiling contribute to privacy violations and abuse;
- o Victims of serious sexual violence (mainly women) are often re-victimised by investigative techniques and need better support;
- o Some communities, such as traveller communities, children, marginalisation of men who had been exposed by data breaches, identified as having unmet needs in data protection and are abandoned by controllers after data breaches. There is a need to raise awareness of the human impact of breaches;
- o 70% of people who have experienced a breach suffer some sort of negative impact, such as loss of employment, loss of empowerment, insecurity and fear. 25% had no support from the organisation that caused the breach.
- o There is a coexistence of privacy and accessibility, noting that privacy supports other human rights;
- o When we talk about personal data protection, we are talking about choices for people that really matter. Choices that will impact their lives and use of data;
- o Indigenous communities face real harms (current and historical) through unauthorised collection of personal data because those communities are often seen as relics of the past;
- o Privacy principles protect individual freedoms and prevent historical abuses like surveillance states.

5. PRIVACY NEEDS TO BE A HUMAN RIGHT AVAILABLE TO ALL.

Privacy harms are evident across global societies. Privacy and data protection laws must be accessible to all humanity:

- o Three common barriers to collecting diversity data: ignorance, fear, and trust issues. Businesses are reluctant to collate this data, together with a fear of backlash and infringing on data privacy as a significant barrier;
- o There is an uneven impact of data privacy on different demographics, particularly women, children, and ethnic minorities;
- o Privacy rights are being about safeguarding people, especially those most impacted by lack of protection;
- o Domestic abuse victims, indigenous communities and people with mental health problems are particularly affected;
- o Understanding local cultures, traditions, and customs in different jurisdictions is crucial to addressing regulatory challenges effectively;
- o Data protection is not just a compliance exercise but a fundamental aspect of humanity, safeguarding individual dignity and enabling agency;
- o The application of data protection principles varies based on cultural, community, and individual factors;
- o Data protection is often associated with significant fines or data breaches in the news, instead of focusing on its meaningfulness in situations without legal protections, where those protections either don't exist, or are inaccessible;
- o There is a lack of discussion internationally on the experiences of original peoples at previous conferences, noting the importance of understanding diverse perspectives;
- o There are challenges of communication and education for indigenous populations which need addressing, and a need for recognition and rights within the broader context of citizenship;
- o There is a lack of recognition of indigenous issues in many countries and a need for frameworks that adequately protect the rights of indigenous groups;
- o Victims of terrorism are exposed to a lack of respect for privacy during a vulnerable time;
- o There are distinct differences in how disabled people are treated in terms of their privacy in comparison to able-bodied people;
- o There is a need for understanding, compassion, and systemic change in how society addresses disability and privacy issues.



6. CAN PRIVACY AND INNOVATION WORK TOGETHER?

It is often said that privacy rules are a barrier to innovation. Here's what our experts said:

- o If you want innovation and prosperity, humans should be seen as inherently special and dignified, rather than tools of the State;
- o It is fundamental for Europe to innovate and integrate AI into new processes;
- o Technology has a dual nature: it can enable but also pose risks to these individuals;
- o Policy makers should use technology to better understand and address regulatory challenges;
- o Indigenous knowledge must be included in AI systems, while also highlighting the risks of misuse and lack of control;
- o Data should serve people, not replace them;
- o There needs to be a cultural shift towards responsible data use and the need for regulators to ensure that data practices align with public interest;
- o Data minimisation is a core principle that supports innovation, competition, and trust in the economy and public institutions. Innovation and competition can coexist with privacy protections;
- o Or alternatively it could be argued that strict data minimisation principles are incompatible with innovation, competition, equity, and practicality;
- o There is a need for a more flexible approach to data collection that allows for innovation and competition, especially for small businesses and can lead to unfair biases and discrimination.

7. HOW DO WE DEAL WITH THE COMPLEXITY OF RULES AROUND INTERNATIONAL DATA FLOWS?

- o It is a priority of the European Union to advance safe and trusted data flows and the importance of protection travelling with the data;

- o There is a need for a set of different mechanisms tailored to specific circumstances, with interoperability and harmonisation a key component among different data transfer schemes;
- o Privacy-enhancing technologies are needed to help facilitate trusted data flows;
- o Adequacy is a comprehensive and significant mechanism for integrating economies and ensuring data protection;
- o Tools like BCRs and certification schemes need to be practical and implementable;
- o Data transfers have an essential role in financial services, with significant impact on personal, business, and trade activities;
- o Optimum operation of economies in the provision of financial services requires instantaneous data flow;
- o Proposed data transfer frameworks could impede data transfers to international organisations, therefore there is a need for flexibility in these proposals;
- o Global data sharing between regulators to combat financial crime and ensure the integrity of financial services is essential;
- o Tools such as Dubai's Ethical Data Risk Index can be used as a guide for organisations to assess the risks associated with data transfers and make informed decisions;
- o Pragmatic solutions are needed to address the challenges faced by developing countries in implementing privacy-enhancing technologies;
- o A principles-based global standard is needed to support the evolving nature of financial services.

8. DO WE NEED TO FOCUS MORE ON PRIVACY CONCERNS AROUND INTERNET OF THINGS (IIOT)?

With major advances in technology around the automotive industry, are we missing an important gap in privacy governance?:

- o Transparency and honesty in data practices is required to address the governance challenge posed by connected cars;
- o The development of IIOT good practice principles is needed to ensure ethical and sustainable use of IIOT systems from the outset of development and strike a balance between adequate privacy and public interest;
- o Car manufacturers face challenges with complying with privacy requirements, which are often compliance-based rather than risk-based;
- o Early transparency about data processing and of privacy labels on cars to inform consumers would reduce risk;
- o Car manufacturers need to consider the long-term consequences of data collection and use, including the potential for unintended consequences.



ACTION POINTS ARISING



INNOVATION:

The conference was advised not to underestimate the long-term impact of technology. We should scan for signals and look for trends, and start asking 'What if?' instead of 'What is?'.

We should also start telling stories... that's how people understand.

We need to collaborate a lot more and as Data Protection Authorities, we need to be more agile to respond to user demand for new technologies.

Data Protection Authorities need to have sensible, pragmatic and flexible interpretations of regulations, and broaden their view to extend beyond personal data.



INDIVIDUAL:

- Consider the potential impact of your actions on human talent and potential.
- Uphold individual rights and contribute to the well-being of the species.
- More education on privacy and online safety is needed in schools, including regular updates on digital literacy.
- Regulators need to start talking to the younger generations and not just about them.
- Investigate the use of self-certification schemes for mental health apps to provide more transparency and user reassurance.
- Explore ways to make it easier for individuals to change their mind and withdraw sensitive mental health data that has been shared.
- Build out a behavioural science team at the regulatory body to better assess the potential harms and benefits of platform design and data sharing practices.

- Increase cooperation between data protection authorities and NGOs to stay informed about emerging technologies and their impact on mental health.
- Explore a unified approach to risk assessment that considers both privacy and online safety.
- Continue multi-stakeholder discussions on topics like age assurance to address overlapping privacy and safety concerns.
- Increase transparency around reporting and addressing of harmful content.
- Enhance digital literacy and empower users to take more responsibility in curating their online experiences.
- Ongoing research, user feedback, and strategic priorities are required to continuously improve and address potential harms.
- Organisations and regulators to take ownership of understanding and managing privacy harms.
- Prioritise data privacy as a basic human right and integrate this view into education policy and business operations.
- Address gender, socioeconomic, and racial biases in data handling, including data privacy risks related to surveillance, harassment, and misuse of sensitive information by government agencies and corporates.
- Build trust across diverse communities that corporate, government, and support agencies will handle data safely and appropriately.
- Promote transparency and consent in data collection, using clear and accessible language in privacy policies, including multiple language translations.
- Evolve internal company cultures to prioritise ethics and privacy in all aspects of data handling.
- Advocate for tech companies to be held accountable for the privacy impact of their products and services.
- Involve diverse community representatives, including those who have experienced privacy violations, in developing data privacy policies and solutions.
- Educate the public, including in schools and workplaces, on data privacy rights to empower people with knowledge and self-advocacy.
- Seek early adopters for the digital privacy charter for schools in Ontario.

- Implement the 3E strategy (Educate, Engage, Empower) for children's privacy education in Hong Kong.
- Advocate for a digital media literacy strategy at the federal and provincial levels in Canada.
- Provide practical support and tools to regulators and innovators globally to implement children's digital rights.
- Conduct a mapping of vulnerable populations (children, disabled, social security) and develop specialised instruments and skills for the agency to respond to their needs.
- Challenge people within the organisation to make communications and guidance more user-friendly, both for industry and individuals, particularly for children.
- Develop better design practices to make choices easy to understand and remove barriers for all users, including children and persons with disabilities.
- Review the age assurance code and consider signing up for it.



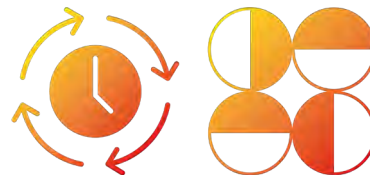
INDEPENDENCE:

- Explore the use of new technologies within DPAs to help manage a complex environment.
- Explore outcome-based collaboration models that leverage behavioural science and technological platforms to address regulatory challenges.
- Develop a culture of collaboration and contextual problem-solving within organisations to navigate the complex regulatory landscape.
- Advocate for digital diplomacy and consider "thinking outside the box" to address the present and future state of digital regulation.



INTERNATIONAL:

- Explore the possibility of mutual adequacy assessments between the EU and other jurisdictions like Brazil, Kenya, and Korea.
- Assess the EU's data protection law for potential equivalency with Korea's data protection regime.
- Revisit the design and implementation of binding corporate rules (BCRs) to make them more practical and globally applicable.
- Encourage more companies to participate in certification schemes like the APEC Cross-Border Privacy Rules (CBPR) system to increase adoption.
- Explore the development of a global, principles-based standard for data transfers in financial services to reduce complexity and challenges.
- Investigate the use of privacy-enhancing technologies, such as federated identity and pseudonymisation, to enable secure data transfers, particularly when working with parties with varying levels of resources.
- Continue to strengthen the collaboration and alignment between financial services regulators and data protection authorities to ensure the effective and compliant flow of data.



INDIGENOUS & INTERCULTURAL:

- Educate businesses and the wider community to stop thinking of data protection as a compliance exercise and start thinking about it in terms of its meaningfulness in situations where people don't have a voice or cannot use it.
- Be careful to consider the cultural, community, and individual factors when applying data protection principles.
- Ensure indigenous communities have a consistent seat at the table in data privacy discussions.
- Develop new principles around data governance for indigenous communities, considering aspects like collective benefits, ethics, and ownership.
- Establish a dedicated working group within the Global Privacy Assembly to specifically focus on the challenges and solutions for protecting indigenous data rights.
- Engage directly with indigenous populations within each country to understand their unique cultural contexts and implement appropriate frameworks and legislation.





INTEGRITY:

- Explore the potential of data trusts and data sharing structures in other sectors beyond cycling, such as the built environment, smart cities, and healthcare.
- Develop methods to better assess and compare data governance practices across different data infrastructures and initiatives.
- Ensure compliance with data protection regulations is seen as an enabler rather than a barrier and use it to build trust in data sharing projects.
- Educate the public on the value of personal data management and the benefits of well-governed data sharing frameworks.
- Establish a multi-stakeholder connected car working group under the Global Privacy Assembly to study and recommend global best practices and standards for connected cars.
- Ensure that data collected from connected cars primarily serves the interests of the people using the cars, not just the interests of the car manufacturers or other entities.
- Consider whether a certain connected feature is truly necessary and proportionate to the user's needs before implementing it in a car.
- Explore the use of "live and smart" labels for connected cars to provide up-to-date information to consumers about data practices, as the technology and data uses may change over time.
- Encourage a cultural shift towards responsible and accountable data practices in the car industry, guided by recommendations and standards, to ensure that connected car technology does not "derail" into unintended and harmful directions.



INFORMATION:

- Work together as data protection authorities, industry, and other stakeholders to find solutions that reconcile privacy protection with innovation and competition.
- Innovate and create a more flexible, interpreted approach to data minimisation that allows for innovation, competition, and equity while still protecting privacy.
- Consider the principle of proportionality when interpreting data minimisation requirements, finding a reasonable amount of data collection rather than strict minimisation or unlimited collection.
- Advocate for changes to the government compensation scheme for victims of terrorist attacks to make it more fair and equitable.
- Encourage the government, media, and regulators to involve more people with disabilities in policy decisions and processes that impact the disabled community.
- Continue to engage with advocates for vulnerable people to provide a voice and fight for the rights and needs of people with disabilities who may not have the strength or ability to advocate for themselves.



LESSONS LEARNED

Organising a major international conference is a complex and multifaceted task requiring meticulous planning, coordination, and adaptability. This section highlights key lessons learned from managing such an event, focusing on planning, logistics, stakeholder management, technology, and contingency planning.

PLANNING AND PREPARATION:

- **Early Planning is Crucial:** Starting the planning process at least two years in advance ensures sufficient time for securing venues, speakers, and sponsors. In this instance we started work on the project as soon as Jersey was awarded the host bid.
- **Clear Objectives and Theme:** Defining the conference's purpose and target audience early helps in curating relevant content and attracting the right attendees.
- **Budgeting and Financial Planning:** Estimating costs accurately and securing funding sources (sponsorships, ticket sales, grants) early is essential for financial stability.

What would we do differently?

Two years would appear ample time to organise an event of this scale. However, given the time required for onboarding of major corporate sponsors, (in some instances onboarding processes took more than 6 months) it would be advisable to start negotiations more than two years in advance, if only at least to cement relationships and ensure the event is secured in the sponsor's calendar.

In terms of the theme, this was established relatively early in the preparations and was therefore not an issue. Content however, and ensuring each session remained 'on theme' was far more challenging. In retrospect, having a wireframe programme in advance of submission of the conference bid may have saved time and energy.

In terms of budgeting, calculating ticket pricing was challenging and is completely dependent on having accurate quotes and/or estimates early on. Planning in a contingency buffer to account for cost of living increases over the period is highly recommended as costs can change between quote and delivery.

VENUE AND LOGISTICS:

- **Choosing the Right Venue:** The venue should be accessible, equipped with modern facilities, and capable of handling international attendees.
- **Catering to International Participants:** Considering dietary restrictions, cultural sensitivities, and language barriers enhances the attendee experience.
- **Transportation and Accommodation:** Collaborating with local hotels and transport providers can offer discounts and ease attendee movement.

What would we do differently?

Given the limited options available in Jersey, finding a primary venue was relatively easy, however consideration must be given to ensuring the venue is fit for purpose. For this event, secure and robust Wi-Fi coverage was essential, however it was not until much closer to the event that it was established that the venue Wi-Fi did not extend to the temporary add on structures, and additional provision needed to be arranged and installed. Given the time again, we would explore this aspect in greater detail during initial scoping of the venue.

The multi-venue requirements off the conference meant that transport to and from the venues and between hotels needed careful consideration. Thankfully, the mix of organised transport arrangements and early engagement of the local taxi companies resulted in a seamless transportation experience for delegates.

Similarly, engagement with local hotels was conducted prior to submission of the bid to ensure there would be sufficient accommodation for 500 visiting delegates. This is peculiar to an Island of Jersey's small size, and I would not expect the same challenges in a larger jurisdiction with bespoke conferencing facilities.

STAKEHOLDER AND SPEAKER MANAGEMENT:

- Engaging High-Profile Speakers Early: Securing keynote speakers well in advance ensures a compelling agenda and higher attendance.
- Effective Communication with Stakeholders: Regular updates to sponsors, speakers, exhibitors, and attendees help manage expectations and avoid last-minute surprises.
- Volunteer and Staff Training: A well-trained team improves efficiency in managing on-site registrations, guiding attendees, and handling inquiries.

What would we do differently?

Perhaps one of the major surprises for the organising team was the significant cost of securing high-profile speakers, some of which explored were quoted at well over £20,000. Therefore, much time and effort was spent on securing low-cost or zero fee speakers, with only a few 'headline' speakers on the programme.

Whilst not something we would necessarily do differently, I cannot over emphasise the importance of engaging a skilled, professional, event management company at the earliest stages of event preparations. Doing so maybe on paper an expensive resource, however the experience they bring with attention to every detail (many of which would not have even been considered) is worth the expense. The close partnership with our own in-house project team enabled us to keep on top of plans at any given moment and without doubt ensured greater efficiency as well as reducing stress.

TECHNOLOGY AND DIGITAL INTEGRATION:

- Reliable Event Management Software: Digital tools for registration, scheduling, and ticketing streamline operations and improving attendee experience. In this instance we utilised Cvent, an event management platform which included the ability for delegates to manage their own experience through an App on their mobile phone.
- Virtual and Hybrid Capabilities: Offering virtual participation options increases accessibility and expands audience reach.
- Strong Wi-Fi and IT Support: Reliable internet access and on-site technical support prevent disruptions, particularly for live-streamed sessions. As mentioned above, this became an issue for us late in project development.

What would we do differently?

Ensuring a positive delegate experience is key to a successful event, and as such, much time and energy was committed at every level in pursuit of this aim. The App was overall a successful addition to the experience, however we did encounter some difficulties engaging with delegates and persuading them to use the App. In retrospect, we could have started this process much earlier and provided delegates with a simple guide to downloading and using the App and choosing their options. It did not however detract from its success as our events team were on hand to assist any delegates who had not provided the essential information we needed.

The Wi-Fi issue has already been detailed above.

MARKETING AND ENGAGEMENT:

- Strategic Promotion: Using social media, email campaigns, and industry partnerships helps maximise attendance.
- Engaging Content Formats: Interactive sessions, panel discussions, and networking opportunities enhance participant engagement.
- Post-Event Follow-Up: Gathering feedback through surveys and maintaining engagement with attendees helps improve future events.

What would we do differently?

If we were to run a similar event in future, we would further promote, via industry partnerships, the fact industry locally was eligible to attend the Open Session.

We recommend engaging with design, marketing and media production partners at the same time as onboarding an event management company, to ensure seamless and streamlined collaboration. It was also extremely important to factor in time for changes to creative content, as responding to feedback from stakeholders, including sponsors, was critical.

RISK AND CONTINGENCY PLANNING:

- Backup Plans for Key Risks: Identifying risks such as speaker cancellations, technical failures, or travel restrictions ensures preparedness.
- Crisis Management Protocols: Establishing clear procedures for handling emergencies, including medical issues and security concerns, is critical.
- Insurance Coverage: Event insurance helps mitigate financial losses from unforeseen circumstances.

What would we do differently?

There are some things you cannot prepare for when organising an international event in Jersey at any time of year, the weather being the most significant unpredictable risk. Fortunately, the 2024 conference was blessed with largely good weather for the time of year, thick fog only arriving the following week. Of course, weather risks were factored into the plans, with the option of remote attendance for speakers and delegates available.

In terms of emergencies, risk mitigation measures were in place with security staff and St John's Ambulance personnel in attendance throughout, and the event was fully insured. Given the extensive risk mitigations in place, there is little that we would do differently.

In summary, organising a major international conference of this scale and diversity requires extensive coordination, proactive problem-solving, and flexibility. Key takeaways include the importance of early planning, stakeholder engagement, digital integration, and robust contingency plans. By learning from these experiences, we hope that future GPA hosts can be well prepared and result in a rewarding conference for all attendees.

SOCIAL MEDIA ENGAGEMENT AND PERFORMANCE



MARKETING AND ENGAGEMENT:

Strategic Promotion: Using social media, email campaigns, and industry partnerships helps maximise attendance.

Making firm decisions about the overall event brand, design and identity at the earliest possible stage, was an essential part of the event's marketing strategy. Planning considerable lead-in time regarding sponsor and speaker updates was also vital and it is recommended that future hosts assess content and deliver a clear, timely and impactful campaign whilst adhering to strict event and sponsor brand guidelines.

The Global Privacy Assembly distribution mailing list proved invaluable when engaging directly with Global Privacy Assembly members and observers and allowed for the provision of early and timely updates and reminders regarding sponsor, programme and speaker announcements, registration, travel, accommodation and instruction about how to download the conference app and book coach transfers, among many more.

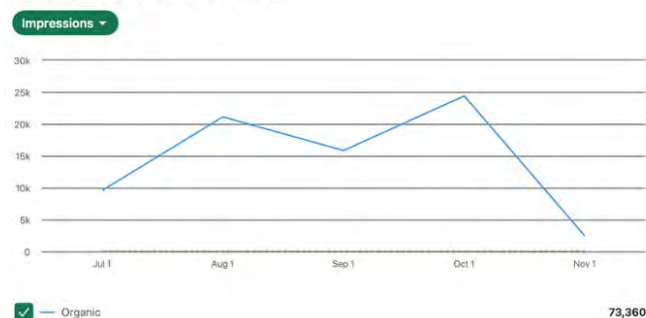
The primary channel we selected to market to our local audience was our Jersey Office of the Information Commissioner LinkedIn channel, accompanied by timely media releases and industry updates via key stakeholders. Conference media releases were distributed to Channel Islands local media as well as relevant industry publications, including the Global Privacy Assembly newsletter. Media releases featuring speaker, programme and sponsor announcements gained the most coverage in the run up to the event and media attendance at the Open Session comprised a mix of local media organisations and industry publications.

SOCIAL MEDIA ENGAGEMENT AND PERFORMANCE:

The conference saw a significant increase in the activity and engagement on the Jersey Office of the Information Commissioner LinkedIn channel in the months leading up to and during the conference.

Impressions represent the total number of times posts have been seen. The chart below highlights the rise in the number of impressions in the third Quarter of 2024 as the conference promotion gained interest, momentum and reach.

Reach of our content

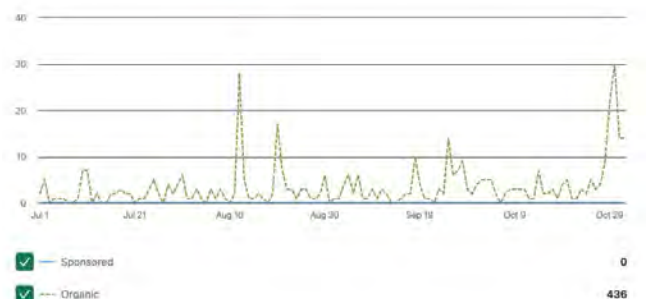


Followers on the JOIC LinkedIn channel increased by 218% from 1 July 2024 to 1 November 2024, an increase of 436 new followers.

Community Growth

2,084
Total followers

436
New followers in the last 124 days
▲ 218.2%



Followers on the JOIC LinkedIn channel increased by 218% from 1 July 2024 to 1 November 2024.

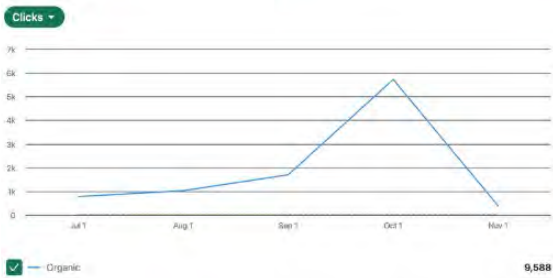
In terms of engagement, LinkedIn 'reactions' increased by 414% to a total of 2,010 during this period 1 July 2024 to 1 November 2024 and the number of comments on our LinkedIn posts during this period increased by 1360%. Content on our LinkedIn channel was reposted 110 times during this period, an increase of 633%.

Interactions

2,010
Reactions
▲ 414.1%

73
Comments
▲ 1,360%

110
Reposts
▲ 633.3%



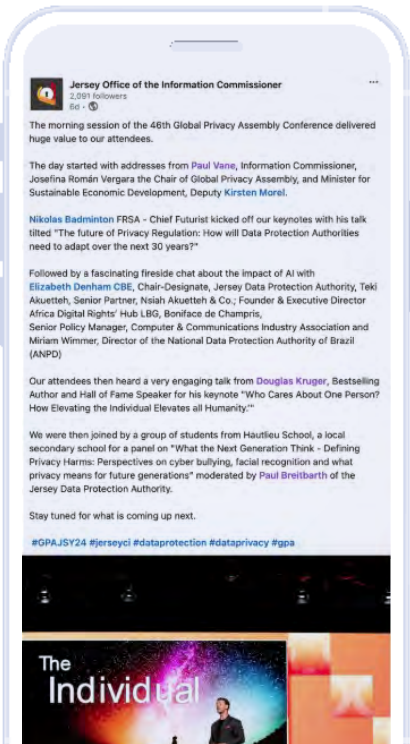
The most popular posts on the JOIC LinkedIn channel during the same period were all created using live content from the Open Session (see the three example posts directly below). Story hooks, engaging imagery and a strong use of Search Engine Optimisation impacted the performance of these posts. Further examples of the content posted live at the Open Session, as well as comments from attendees, can be seen further below. Speakers and sponsor organisations were tagged on LinkedIn whenever possible to encourage the sharing of content among their networks.



66.4% ENGAGEMENT



58.47% ENGAGEMENT



56.43% ENGAGEMENT



LOCAL ECONOMIC IMPACT

A key objective of hosting a major international conference such as this was to create a significant financial injection to the local economy during what is usually a quiet period for local tourism, hospitality, retail and the transportation industry.

Some of the key economic effects observed during the conference week are detailed below.

1. INCREASED TOURISM AND HOSPITALITY REVENUE

The large influx of international and domestic visitors led to higher occupancy rates in the major hotels, with increased bookings over and above what would normally be expected during October half term week. The conference created a noticeable buzz around the town hub of St. Helier with greater demand for restaurants, cafes, and entertainment venues. This was no doubt a welcome boost in revenue for the hospitality sector.

2. JOB CREATION AND BUSINESS GROWTH

The demand for bespoke and expert event planning, security, transportation, and other logistical services created direct and indirect employment opportunities. Local businesses were used as much as possible, with catering companies, printing services, digital creators and technology providers benefitting from the increased demand.

3. TRANSPORTATION AND INFRASTRUCTURE UTILISATION

Public transportation systems, taxis, and rideshare services experienced a surge in usage, increasing fare revenues. In addition to the services of a local coach service who provided the bulk of the transport during the conference week, local taxis and public buses were well-utilised, with taxi companies in particular commenting on increased revenues.

4. INCREASED RETAIL SPENDING

Conference attendees often spend on shopping, souvenirs, and other local goods, providing a boost to retail businesses. The Jersey conference was no exception in this regard, with many retailers commenting on the increased footfall and sales across the week. Additionally, local artisans and vendors were provided opportunities to showcase their products through delegate goody bags.

5. LONG-TERM ECONOMIC AND INVESTMENT BENEFITS

A successful international conference enhances the host nation's global reputation, potentially attracting future tourism, business investments, and further international events. This long-term branding can lead to sustained economic benefits. Feedback from conference delegates demonstrated a desire from many to return to the Island for a holiday in the future.

6. GOVERNMENT AND TAX REVENUE GAINS

Higher spending from attendees translates into increased sales tax revenue for local government, which can be reinvested into public services and infrastructure. Additionally, licensing fees and permits for vendors contribute to municipal earnings.

In summary, while hosting a major international conference requires upfront investment in logistics and infrastructure, the success of the GPA 2024 Conference in Jersey shows that the economic benefits can greatly outweigh the costs. By boosting local businesses, particularly during the usual tourism shoulder months, creating jobs, and enhancing the Island's international profile, such events can serve as a powerful catalyst for productivity and economic growth.



DELEGATE FEEDBACK

Of those that responded to our optional post-event survey:

85% SAID THE CONFERENCE THEME ADDRESSED CURRENT TRENDS AND CHALLENGES IN PRIVACY AND DATA PROTECTION VERY OR EXTREMELY EFFECTIVELY

83% SAID THE CONFERENCE SESSIONS WERE VERY OR EXTREMELY USEFUL IN PROVIDING NEW INSIGHTS AND PROMOTING POSITIVE CHANGE IN PRIVACY AND DATA PROTECTION

95% RATED THE OVERALL QUALITY OF THE SPEAKERS AND PANEL MEMBERS AS VERY OR EXTREMELY GOOD.

83% SAID THE CONFERENCE SUCCEEDED VERY OR EXTREMELY WELL IN FOSTERING A DEEPER UNDERSTANDING OF THE CULTURAL AND BEHAVIOURAL CHANGES NEEDED AROUND THE USE OF PERSONAL DATA

80% SAID THE NETWORKING OPPORTUNITIES WERE VERY OR EXTREMELY EFFECTIVE IN HELPING DELEGATES CONNECT WITH OTHER PROFESSIONALS AND EXPAND THEIR NETWORK

APPENDIX



APPENDIX 1: FULL SPEAKER LIST

SPEAKER	TITLE
Akuetteh, Teki	Africa Digital Rights Hub
Anchorena, Beatriz	AAIP Argentina Director
Antonipillai, Justin S.	Founder and CEO, Stewardshipped.ai & Senior Advisor - Gretel
Artz, Vivienne	Senior Data Strategy & Privacy Policy Advisor to the Centre for Information Policy Leadership
Asai, Yuji	Commissioner, Personal Information Protection Commission (PPC) Japan
Badminton, Nikolas	Futurist
Baker, Lori	Director of Data Protection, Dubai International Finance Centre Authority
Barrington-Leach, Leanda	Executive Director, 5Rights Foundation
Bedoya, Alvaro	Commissioner, Federal Trade Commission
Bellamy, Bojana	President, Centre for Information Policy Leadership
Benn, Cari	Associate General Council, Microsoft
Blackmore, Davida	Principal (AdvocateDVB) and Chairman of the Mental Health Review Tribunal (Jersey)
Botterman, Maarten	Director, GNKS Consult BV
Breitbarth, Paul	Jersey Data Protection Authority
Britton, Jill	Director General, Jersey Financial Services Commission
Caprio, Dan	Co-Founder and Chairman, The Providence Group
Cave, Jonathan A.K.	Academic Economist and Associate at GNKS
Colclasure, Sheila	Global Chief Data Integrity and Public Policy Officer
Coxshall, Mark	Chief Executive Officer, EyeCan
Crompton, Malcolm	IIS Partners
de Champris, Boniface	Computer & Communications Industry Association, Brussels
Denham CBE, Elizabeth	Chair, Jersey Data Protection Authority
Denis, Marie-Laure	Chair of the Commission Nationale Informatique & Libertes (CNIL)
du Marais, Bertrand	Commissioner, CNIL

SPEAKER	TITLE
Dufresne, Philippe	Commissioner, Office of the Privacy Commissioner, Canada
Edwards, John	Information Commissioner, UK ICO
Falle, John Henry	
Gerlach, Natascha	Director for Privacy & Data Policy, Centre for Information Policy Leadership
Girod, Clarisse	Acting Head, Division on Data Flows, Governance and Privacy, OECD
Hall, Wendy Dame	Regius Professor of Computer Science, University of Southampton
Hardinges, Jack	Independent Consultant, Foresight
Harker, Rachel	Technology Development Consultant, Digital Jersey
Hodges, Christopher OBE	Chair, Regulatory Horizons Council; Emeritus Professor of Justice Systems, Oxford University
Holloway, Dan	CEO & Founder, Rogue Interrobang
Horvath, Jane	Partner, Gibson, Dunn & Crutcher
Hughes, Trevor	CEO, IAPP
Ismail, Noriswadi	Senior Director of Data Privacy, GSMA
Johnson, Matthew	Director of Education, MediaSmarts
Jones, Joe	Research Director, IAPP
Kassait, Immaculate	MBS, Data Commissioner / 1st Vicechair, Network of African Data Protection Authorities (NADPA)
Keaney, Emily	Deputy Commissioner, UK ICO
Kidron OBE, Beeban Baroness	Member of the House of Lords, Founder & Chair 5Rights Foundation
Kind, Carly	Privacy Commissioner, Office of the Australian Information Commissioner
Ko, Haksoo	PIPC Korea
Kohnstamm, Jacob	Former Chair, Jersey Data Protection Authority
Kosseim, Patricia	Privacy Commissioner for Ontario, Canada
Kruger, Douglas	International Inspirational Speaker
Lai, Joyce	Assistant Privacy Commissioner for Personal Data (Corporate Communications and Compliance) PCPD
Lang, Carolyn	Pinsent Masons
Lisievici Nevin, Andreea	Privacy Digital and AI Consultant, Trainer & Mentor, Privacy Craft
Lorenzo, Yukiko	Senior Vice President, Assistant General Counsel, Privacy and Data Protection, Mastercard
Marelli, Massimo	Head of Data Protection Office, International Committee of the Red Cross (ICRC)

SPEAKER	TITLE
Massé, Estelle	Policy Officer, International Affairs and Data Flows, Directorate-General for Justice, European Commission
Morel, Kirsten	Government of Jersey Minister for Sustainable Economic Development
Morgan, Shana	Global Head of Privacy & AI Legal Compliance, L3Harris Technologies
Nester, Jade	Director, Data Public Policy, Europe, TikTok
Phippen, Andy	Professor, Bournemouth University
Polonetsky, Jules	Chief Executive Officer, Future of Privacy Forum
Purcell, Richard	CEO, Corporate Privacy Group
Race Brin, Katherine	Chief Data Privacy Officer, The World Bank
Redmond, Emma	Associate General Counsel, Head of Privacy and Data Protection and Ireland Site Lead for OpenAI
Reynders, Didier	Commissioner, European Commission
Román Vergara, Josefina	Chair, Global Privacy Assembly & Commissioner, Mexico INAI
Schrepel, Thibault	Associate Professor of Law at the Vrije Universiteit Amsterdam, Faculty Affiliate at Stanford University
Scott, Moz	Assistant Minister for Sustainable Economic Development, Government of Jersey
Talus, Anu	Chair, European Data Protection Board (EDPB)
Tan, Steve	Partner, Rajah & Tann Singapore
Vane, Paul	Jersey Information Commissioner
White, Alexander	Privacy Commissioner, Bermuda
Wiewiorowski, Wojciech	European Data Protection Supervisor
Wimmer, Miriam	Director of the National Data Protection Authority of Brazil (ANPD)
Wright, Kate	CEO, Freeda
Wright, Martine	7/7 survivor, Paralympic athlete, Inspirational and Motivational Speaker
Zanfir-Fortuna, Gabriela Dr	Vice-President for Global Privacy, Future of Privacy Forum

APPENDIX 2: SPONSORS

GOLD
Google
IAPP
Apple
Johnson & Johnson
Government of Jersey
SILVER
Microsoft Corporation
Meta
Merck Sharp & Dohme LLC
Gen II
Open AI

BESPOKE
HP Inc
TikTok UK
ZoomInfo Technologies LLC
Visit Jersey
SIDE EVENT
Centre for Information Policy Leadership
EXHIBITOR BOOTH
Calligo
GSMA Limited
Jersey Cyber Security Centre
Digital Jersey

APPENDIX 3: FINANCIALS

Not only did the conference provide a platform for important data protection discussions, it also had a positive economic impact on local businesses which was distributed across several sectors.

The hospitality industry benefited from the delegates staying in local hotels and dining at local restaurants, coupled with local suppliers supporting the conference with everything from event management and logistics through to the catering services received.

The Conference was primarily funded through two revenue streams: Ticket sales and Sponsorship.

The combination of these two sources of funding provided a good financial foundation making the conference financially viable while also ensuring a good experience was had by the delegates and key stakeholders who were in attendance.

The funding raised covered the operational costs of the event which included venue hire, the technical infrastructure, speaker costs and logistics. The ticket sales and sponsorship made the event financially feasible.

Whilst the conference numbers are still being finalised at the time of writing this report, the total income generated from tickets sale and sponsorship vs the associated conference expenses has resulted in a near breakeven outcome.

Conference Financial Summary 2024

Ticket Sales	£285,855
Sponsorship received	£478,998
Total Income	£737,853
Total Expenditure	£718,208

APPENDIX 4: WITH THANKS TO...

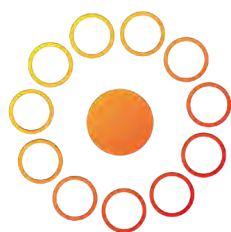
It was a pleasure to welcome our attendees to Jersey. A special thank you to all of our speakers, sponsors, GPA Members and delegates, as well our event management partners 3D Events, design partners STS Graphics and the Global Privacy Assembly Secretariat (Mexico INAI) for their expertise and guidance from the very beginning. Also a big thank you must go to Commissioner Alex White from Bermuda for his insights and experiences as the conference's previous host, and to the Programme Advisory Committee for their wisdom and technical expertise in producing an excellent conference programme.

Thank you to:

- Acolad group
- ArtHouse
- Blue Llama
- Cvent
- Delta Events
- ITV's Jess Dunsdon
- Eden by Claire
- Elite Security
- actor John Henry Falle
- Floor Ten Agency
- Focused IT
- Grand Hotel
- H20
- Harpers Catering
- Hotel De France
- Darren Huelin Photographer
- iMAG
- local events band Inside Job
- Jersey Fudge
- Jersey Heritage
- Jersey Honey
- Jersey Kitchen
- Jersey Maritime Museum
- Jersey Telecom
- La Mare Wine Estate
- Marquee Solutions
- PBS Group
- Pomme d'Or Hotel
- Master of Ceremonies Richard Purcell
- Royal Jersey Showground
- The Radisson Blu Waterfront Hotel
- The Royal Yacht Hotel
- Slingshot Films
- Stage 2 Productions
- St John's Ambulance Jersey
- Tantivy Coaches

A huge final thank you must go to my incredible team at the Jersey Office of the Information Commissioner for their commitment, dedication, hard work and a huge team effort helping to deliver an event which showcased the very best of Jersey and produced a spectacle that we will all remember for years to come.







GPAJERSEY.COM