All-Party Parliamentary Group on Artificial Intelligence

International Association of Privacy Professionals

From Digital Entropy to Digital Responsibility

The Future of Digital Policy and the Importance of Professionalisation

BIG INNOVATION CENTRE
Secretariat

13 March 2025
Policy Forum

Table of Contents

Title: From Digital Entropy to Digital Responsibility: The Future of Digital Policy and the Importance of Professionalisation
Authoring Organisation: All-Party Parliamentary Group on Artificial Intelligence (APPG AI)
Date of Publication: March 2025
Publication Type: Parliamentary Brief | Policy Brief
Publisher: Big Innovation Centre

INTRODUCTION

This document is a 'creative transcript' and summary of an APPG AI - IAPP special meeting that took place on 13 March 2025 in the House of Lords Committee Room 2a, UK Parliament. It exclusively contains crucial discussion elements; not all points are addressed.

DETAILS

- APPG AI - IAPP Special Meeting: From Digital Entropy to Digital Responsibility: The Future of Digital Policy and the Importance of Professionalisation
- Time 5:30 pm – 7:00 pm (GMT)
- Date: Monday, 13 March 2025
- Venue: Committee Room 4a in the House of Lords.

CONTACT THE SECRETARIAT

appg@biginnovationcentre.com
APPG AI Secretariat
Big Innovation Centre

PANELLISTS

- **Trevor Hughes**: CEO & President, IAPP
- **Joe Jones**: Director of Research & Insights of the IAPP

INSIGHTS GIVERS

- **Isabelle Roccia**: Managing Director, Europe, IAPP
- **Lara Liss**, Chief Privacy and Data Trust Officer, GE HealthCare
- **Janine McKelvey**, General Counsel - Group Data Privacy & Ethics Officer at BT
- **Simon McDougall**, Chief Strategist, Privacy and AI, at ZoomInfo

MEETING CHAIRS AND RAPPORTEUR

The Meeting was co-chaired by **Allison Gardner MP** and **Lord Clement-Jones CBE;** Co-Chairs of the All-Party Parliamentary Group on Artificial Intelligence.

Rapporteur for this meeting: **Professor Birgitte Andersen**, CEO Big Innovation Centre

Aim of Session

From Digital Entropy to Digital Responsibility: The Future of Digital Policy and the Importance of Professionalisation

This APPG AI – IAPP Special Meeting focuses on the future of digital law and policy. It examines the growing social, technical, regulatory, and organizational responses necessary for the responsible development and use of digital technologies. We will explore the idea of Digital Entropy—how chaos and unpredictability in digital systems impact governance. The discussion includes how policymakers, regulators, and industry collaborate to manage risks across different digital domains. Key topics also include the role of professionals, such as AI governance specialists, and the emerging regulatory and organizational frameworks that support responsible digital innovation.

Questions raised to inspire the discussion:

- What are current or anticipated examples of complementary digital laws and policies objectives and what are examples of digital laws and policies that are or might be in tension?
- What are some of the most pressing and most complex digital policy and governance risks that exist?
- What structures, practices, and approaches can help organisations cohere and coordinate across the matrix of digital law and policy?
- How do we build and scale the capacity and capability of skills in digital governance to encourage better, safer, and more responsible use of digital technologies?

Above (from left to right): **Professor Ashley Braganza** (Dean, Brunel Business School), **David Elcombe** (CEO WindWorkX), **Yogesh Joshee** (CEO, GenAirate Technologies), **Simon McDougall** (Chief Strategist, Privacy and AI, at ZoomInfo), **Isabelle Roccia** (Managing Director, Europe, IAPP), **Joe Jones** (Director of Research & Insights of the IAPP), **Janine McKelvey**, General Counsel (Group Data Privacy & Ethics Officer at BT), **Lord Clement-Jones CBE** (APPG AI Co-Chair), **Lara Liss** (Chief Privacy and Data Trust Officer, GE HealthCare), **Professor Birgitte Andersen** (CEO Big Innovation Centre and APPG AI Secretariat), **Trevor Hughes** (CEO & President, IAPP), **Allison Gardner MP** (APPG AI Co-Chair), **Lord Holmes MBE** (House of Lords), **The Earl of Erroll** (House of Lords), **Lord Taylor of Warwick, Sarah Reynolds** (Partner, EY Law), **Esra Kasapoglu** (Executive Director of AI and Data Economy, Innovate UK - UKRI).

FINDINGS

ACTION FIELDS FOR POLICY AND STAKEHOLDER GROUPS

(1) Summary of Speakers’ Statements and Action Points for Stakeholders:

Education and Training:

Invest in Education and Professional Development:

- Support educational initiatives that embed data protection, ethics, and AI governance across various disciplines.
- Promote continuous professional development programs for current employees to ensure they are up to date with the latest regulatory requirements and best practices in AI governance.

Industry Challenges:

Promote Cross-Sector Collaboration:

- Work collaboratively with regulators, industry peers, and educational institutions to develop harmonised policies that reduce conflicts and provide clear guidance.

Anticipate and Manage Future Challenges:

- Prepare for rising expectations regarding AI's role in decision-making and potential consequences from its use.

Recognise the Commercial Value of Governance:

- View effective AI governance not just as a regulatory necessity but as a critical factor for commercial success and competitive advantage.

Governance:

Enhance Trust through Transparency:

- Foster transparent practices regarding data provenance and usage to build trust with clients and stakeholders.

Establish Robust AI Governance Frameworks:

- Implement and maintain comprehensive AI governance frameworks that outline clear roles, responsibilities, and protocols.

Proactively Engage with Regulatory Changes:

- Stay informed about emerging regulations and actively participate in discussions to ensure compliance and mitigate risks.

Implement Practical Tools for Governance:

- Utilise technology, such as AI-driven chatbots, to streamline governance communication with customers, ensuring clarity in practices.

By incorporating professional development into the actions for stakeholders, this approach highlights the necessity for continuous learning and skill enhancement to effectively navigate the complexities of AI and data governance.

(2) The Q&A and discussion following the presentation statements highlighted new points and their implications.

Education and Training:

Importance of Professional Skills & Standards

- The panel emphasises the need for professionalised oversight, auditing, testing, and risk assessment in AI. There’s a focus on developing and harmonising standards across jurisdictions to ensure interoperability and safety. The IAPP’s efforts include certifications with thousands of trained professionals.

Need for Professional Qualifications & Interoperability

- Creating recognised professional certifications and qualifications is essential. There’s a challenge in aligning standards across different countries’ education and professional systems to facilitate international cooperation and skills transfer.

Training for Broader Professions

- As digital technology becomes integral to various professions, it’s important for lawyers, doctors, teachers, and other professionals to develop basic digital issue-spotting capabilities. This is necessary for maintaining trust, safety, and making informed decisions.

Governance:

Regulatory Gaps & Governance

- There’s concern about gaps in governance, especially in the UK. Questions arise about whether there should be a statutory requirement to govern AI and who should be the regulator, especially for systems used in healthcare and public services.

Industry Challenges:

Resource Constraints for Investing in Expertise:

- Smaller companies face difficulties due to high costs of expertise and lack of skills. There’s a risk they might avoid compliance or fail to adopt responsible AI practices. The need for accessible guidance, testing frameworks, and support to help all industry players is highlighted.

Balancing Regulation and Competitiveness

- Companies need to navigate how legislation can be used as either a shield or a sword. They should leverage legislation for competitive advantage while ensuring responsible AI deployment. International examples (like Singapore) show proactive regulation and testing efforts to support industry growth.

Balancing Regulation and Innovation

- The overarching goal is to enable UK businesses to succeed in AI, balancing regulation with innovation, and ensuring that responsible AI practices are accessible and affordable across the industry.

(3) The stakeholders in the outlined action points above include, in no particular order:

Policymakers – government officials and legislators shaping the regulatory framework for digital technologies.

Regulators – agencies and authorities responsible for enforcing compliance and overseeing digital risk domains.

Industry – technology companies, digital service providers, and industry organisations developing and deploying digital technologies.

AI Governance Professionals – specialists focused on guiding responsible AI development and implementation.

Organisational Leaders – executives and decision-makers within corporations managing digital transformation.

Legal Experts and Lawyers – professionals advising on compliance, risk, and legal implications of digital policies.

Academics and Researchers – studying socio-technical impacts and proposing future policy directions.

End Users and Society – individuals and communities affected by digital technologies and policies.

International Bodies – organisations involved in global digital policy standards and cooperation.

Panellist:
Trevor Hughes

Panellist:
Joe Jones

Insights Giver:
Isabelle Roccia

Insights Giver:
Lara Liss

Insights Giver:
Janine McKelvey

Insights Giver:
Simon McDougall

EVIDENCE

APPG AI Chair:
Allison Gardner MP

APPG AI Chair:
Lord Clement-Jones CBE

Secretariat & Rapporteur:
Professor Birgitte Andersen

Joe Jones

Director of Research & Insights
IAPP

Welcome: I am Joe Jones, the Director of Research and Insights at the IAPP. We are genuinely excited to discuss digital entropy and the energy that is currently in action to bring order to the disorder in digital law, policy, and governance. Together, we will walk through the issues as we see them, shining a light on the practices as they are developing and merging.

Navigating the Dynamic Legal Landscape: I want to take you on a brief journey through the vibrant and ever-evolving landscape of UK law and policy as it relates to digital technologies. From the UK Data Protection Act and GDPR to the recent passage of the Data Use and Access Bill, the Online Safety Act, and the Digital Markets Regime, we see a legislative environment rich with innovation, regulation, and opportunity.

The 'Alphabet Soup' of Regulation: But this environment is often described as an "alphabet soup" — a myriad of laws and frameworks that shape how organisations operate in the digital age. It's complex, yes, but also vital. Navigating this landscape requires understanding and agility.

The Power of Collaboration and Regulatory Evolution: Central to this effort are our regulators. They are actively working to move beyond silos, fostering greater coordination and cooperation across different domains. This shift toward a more connected approach is essential to managing the increasing complexity of our digital ecosystem.

Unified Efforts for a Shared Vision: And this movement is reflected not only within government and Parliament, but also within industry itself. As I see it, collaboration is the key to addressing what I call "digital entropy" — the disorder created by rapid technological change.

Looking Ahead: Building Order from Chaos: Looking ahead, I am excited about the discussions we have with our industry leaders. They will now share how their organisations are responding to these challenges — working to bring order to chaos and to shape a responsible, innovative digital future. First you will hear from our CEO and President, Trevor Hughes, who will introduce the IAPP, our mission, our and work.

Trevor Hughes

CEO & President
IAPP

I want to introduce both the IAPP (The International Association of Privacy Professionals) and the work that we do, and then some thoughts about this moment that we have described as digital entropy. Entropy, of course, is a state of disorder, and I'll talk about that and hopefully offer a hopeful solution to all of this, an opportunity for us to see a path forward.

About the IAPP

The IAPP is a global professional association. We were founded 25 years ago. We're celebrating our 25th anniversary this year. We have 88,000 members in 150 countries around the world. I am delighted to say that our second largest country in terms of population of members is here in the UK. We are notably policy neutral. We are not a lobbying or campaigning body. We are a professional association with a mission focused on building the professionals who do the work of digital policy.

Our formation, our origin, is in privacy and data protection, and certainly the majority of our members work in those domains, but we have broadened to include AI governance, cybersecurity law and other intersecting domains, of which there are more and more from areas of digital policy.

A Historical Perspective on Privacy and Technology

Before I get into a conversation about AI and the moment of AI governance that we find ourselves in, I'd like to turn to history and offer a lesson that I think we have from some of the earliest days of technological innovation and thinking about privacy, particularly in the intersection with the law.

In 1892, law partners in Cambridge, MA, Louis Brandeis, who famously went on to serve on the US Supreme Court, and Samuel Warren, who was his law partner, both graduates of Harvard Law School, were reflecting on a technological innovation that was greatly challenging their understanding of privacy and society at that moment. That technological innovation seems almost quaint today. It was not photography, but flexible film. Photography had been around for some time. But flexible film had actually changed the nature of photography. It had allowed cameras to become quite small, portable and actually concealable. And so all of a sudden photos could invade privacy in quite a significant way.

Brandeis and Warren, being Harvard Law School graduates and practising lawyers, at that point, wanted to respond to the privacy violation associated that they felt associated with this new technology, and so they did what they would do. They wrote a law review article. It's called the "Right to Privacy." I recommend it to you all. It was published in 1890 in the Harvard Law Review.

And what they said in that law review article, I think, is quite notable, and that is when technology changes, so too must the law. When technology changes norms in society, when technology changes expectations in society, when technology creates new harms that were unforeseen before that innovation, so too must the law evolve, innovate, and change to respond to that. In fact, the quote is really quite good and it would be contemporary or make just as much sense in our arguments today.

So they said in the law review article, "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person." And that is the right to be let alone. They argued for the right to privacy to be created. Much of our privacy law derives from this original law review article by Brandeis and Warren. So as tech innovates, so too must the law.

The Evolution of Digital Governance

But as the law evolves, we have to build the structures that give life to the law, and that's the place where the IPP works. The resources, the technology, the professionals, they make real, they operationalise these new legal standards and respond to the challenges of technological innovation.

I mentioned the IAPP is celebrating our 25th anniversary this year. When we were formed, we had less than 300 members. There were very few privacy professionals around the world. Fast forward to today, we have 88,000 privacy professionals doing the incredible work of navigating yes, privacy compliance but more broadly than that, engendering trust within organisations, both in the public and the private sector, with how organisations use our data.

Let me give you a sense of that growth, not from our membership growth, which I think is significant but in terms of the growth of the law. Just five years ago, January of 2020, the research firm Gartner estimated that 10% of the world's population was subject to an overarching comprehensive privacy law that includes the UK under the GDPR at that moment in time. The GDPR was part of that, along with Singapore, Japan, Hong Kong, Australia, New Zealand, Canada—many, many jurisdictions had privacy laws in place, comprehensive privacy legislation, but it was only 10% of the global population. Fast forward to January of this year, Joe and his team redid that research and we looked at how much of the global population is subject to a comprehensive national privacy law. The figure is now 82%. So in five years, 72% of the world's population has had a novel, innovative, brand new privacy law put in place. That creates an enormous amount of work inside organisations, and we have seen a commensurate growth of the profession around the world to respond to the demands of those laws globally.

The Accelerating Pace of Change in AI

What we find today, though, in this era of AI, is that the pace of change is accelerating. Let me speak to that just a little bit. AI, like so many other innovations before, has mediated our social norms. It has mediated our standards. It has created new theories of risk and harm that must be addressed.

There are a few key characteristics here. One, the pace of this change, I think, is quite notable. AI has been adopted faster than many other technologies in the past, and it seems almost dizzying today that we have a new AI innovation emerging almost daily. Really, we have legacy policy issues that we can easily recognise within AI systems today. So there are legacy issues of privacy and intellectual property. There are issues of consumer safety that we can recognise given our existing legacy standards, our laws that we know how to apply.

But there are also novel issues, issues of algorithmic discrimination, issues of bias within the system, even issues associated with transparency around decision-making within these AI systems. The IAPP sought this, and that intersection between privacy and AI has existed for the entire history of the IAPP. Our conferences, our publications have always had content and sessions related to the intersection of AI and data technology and privacy standards. But about three years ago, we began to see quite a significant change; sessions in our conferences had more people attending. There were more clicks on articles associated with AI in our publications, and clearly something was happening.

Certainly, the launch of ChatGPT-3 just two years ago now, not even, seems to have been a watershed moment, I think, in the broad social discourse on AI. And so the IAPP launched an AI programme. We created an AI governance centre, we launched a conference, we created a certification, and a training to begin the work to professionalise those who will be doing the work of AI governance, AI ethics, and responsible AI inside organisations.

In order to take that development out to the world, we knew that we had to share the story and so myself, Joe, and others at the IP got on the road. We were here in London meeting with Lord Clement Jones and others. We were in Brussels and Paris and Munich. We were in Ottawa and Washington DC, we were in Sydney and Singapore and Hong Kong. We were in many places around the world. And as we talked to governmental policymakers, to regulators, as we talked to industry and organisational leaders, a very common story kept repeating itself and that was organisations felt a state of disorder within their organisations as they were trying to navigate digital policy.

Challenges of Navigating AI Policy

They were struggling with the number of issues that AI was raising, and let's be clear, AI is not in a neat and tidy box as a policy issue. It brings in privacy issues and competition issues and intellectual property issues and consumer safety issues and discrimination issues. It encompasses a number of issues, and the challenge inside many organisations, both in the public and private sector, is that those policy issues have largely been dealt with within silos. And those silos do not interact, and they're not within a common framework of organisational structure.

So from a risk management perspective, what we found was that there was a lack of structure. This was well said by actually a leader here in London when I was speaking to him about exactly this issue. His response to me was, and he was the privacy and AI leader for his organisation, "It's as if I am a medical professional and I'm in an operating theatre with other medical professionals and we're all operating on the same patient. There's an anaesthesiologist, a nurse, a doctor, surgeon, whoever might be there, but none of us are allowed to talk to each other. We all speak different languages. We all want the best outcome for the patient, but we are all speaking different languages."

We came back to the office, Joe and I and others shared these stories and we realised that there was something there, that there was something that we were seeing in the broad global— and I won't say marketplace because it was both public and private sector. We realised that there was something important for us to capture.

We thought about it a bit and realised that we could capture it with this idea of entropy, which is the second law of thermodynamics, and it suggests that all systems head toward disorder. That is a deeply depressing law of physics. I think that all systems head towards disorder. Entropy indeed is what we found—a state of disorder inside organisations.

Joe's team led research for us, and this is that research. It's actually available on our website. Our organisational digital governance report is the result of both qualitative and quantitative research that we did from interviews and surveys of a number of organisations within the IUP membership. What we were trying to capture is how are you structuring these issues today? How are you responding to these issues? What, given the technological innovations and the legal innovations that we are beginning to see, and the social norm disruption that is clearly occurring, what are the organisational responses being taken by organisations in the public and private sectors to deal with these new dynamic issues?

What we found was exactly that matrix—an intersecting matrix of complex digital policy silos where issues of data, technology, and human interest, ethics, law, policy all intersected across many different domains, and those domains do not have a common framework for organisational management. Those frameworks are struggling at this point. Boards and executives are struggling with how to manage those issues.

We also documented a maturity model for three different stages, and I should note that at the very highest stage of the maturity model, we found very few organisations—very few organisations would capture or would describe themselves as being at a high state of maturity for their overall digital governance response.

Meeting the Challenges of Today's Environment

And so we are at the IAPP in the midst of an enormous lift, a global lift of trying to create the professionals, to create the tools and resources that they need to respond to the entropy of this moment. Some of you will know the J.M.W. Turner painting here at the National Gallery, "The Fighting Temeraire." It's one of my favourite paintings, and I try to visit it whenever I'm in London. That reflects a moment that I think is evocative of the time we find ourselves in.

The reason that painting is so emotional, so compelling, is not only Turner's amazing technique; it's not merely the colour palette he uses, all of which are masterful. It's that it is an image that represents the transition in the industrial era, from the age of British sail to the age of steam. The Fighting Temeraire is one of Nelson's fighting ships, fought in the Battle of Trafalgar, and it's being hauled away to scrap. Simon Schama, the noted art historian, called this painting a representation of the turbulence of a transitional age.

And I think we find ourselves in a turbulent transitional age today. We are in a crucible of policy; innovations are being developed around the world as we speak. There are many dozens, if not hundreds, of AI policy initiatives that are being proposed around the world. Clearly, the EU AI Act is having a significant influence, but we have seen laws introduced and passed in states within the United States. South Korea has a major standard underway. There are standards being introduced and proposed all around the world, yet we still have a lack of organisational structure to respond to many of those standards.

We also have a lack of people to do the work. I noted at the beginning that one of the characteristics of AI is the pace of change. The pace of innovation is quite challenging. It has taken the IAPP 25 years to go from 300 members to 88,000 members around the world, and I would argue that that is still insufficient to respond to the data protection work that we were originally formed to address. AI is on an even faster timescale, and we need professionals even more quickly than that.

The Need for Upskilling in AI Governance

But here's the challenge: these professionals, these AI governance professionals, actually don't exist because all of those digital policy domains come together in AI governance and AI standards. To find someone who is an expert across cybersecurity, data protection, AI governance, algorithmic discrimination, consumer protection, and risk and safety—that's a unicorn. We will not find that person.

So what do we do? We need many, many people around the world to upskill to become able to respond to the challenges that we see with AI, to make these technologies safe and trustworthy so they can be implemented and fulfil their greatest purpose in society. We need to bring people laterally across. We need to upskill existing professionals.

Our membership, largely, is being given the portfolio of AI governance and risk management. We have data to support this: in over 50% of organisations, the file labelled "AI risk" is being handed to the data protection or privacy leader. We have some of them here to talk to you tonight. In over 80% of our membership responding to our survey, they said that issues not related to privacy—AI issues—had been added to their desks in the past two years.

Our members globally are largely being asked to respond to these issues, but so are cybersecurity professionals, as well as trust and safety and content moderation professionals. Many others are as well. Our moment to upscale those professionals is now. We need tens of thousands, if not hundreds of thousands, of these professionals globally to ensure that these technologies work effectively.

How to Address the Moment of Entropy

So what do we do, or how do we respond to this moment of entropy? Well, the good news is that the second law of thermodynamics is not an immutable law. There is actually a way to fight back against entropy, and that is the introduction of new energy into a system. We need to introduce new energy, new innovation from the policy perspective, and new ranks of professionals who have been upskilled to deal with the complex issues associated with AI in society.

We need to introduce new energy into this broad policy domain again so that we can ensure that AI meets our human needs and provides the greatest benefits that this technology promises while reducing the harms that could possibly arise.

Thank you.

Summary of Trevor Hughes's Key Points and Actions for Stakeholders

1. Introduction to the IAPP:
   - The International IAPP (Association of Privacy Professionals) is a global professional association celebrating its 25th anniversary with 88,000 members across 150 countries.
   - It aims to build professionals in digital policy, focusing on privacy and data protection while expanding into areas such as AI governance and cybersecurity law.
2. Historical Reference:
   - The evolution of privacy law is evidenced through the work of Louis Brandeis and Samuel Warren in the late 19th century, who argued that as technology evolves, so must the law.
   - Their publication, "The Right to Privacy," underlines the necessity for legal frameworks to adapt to technological advancements.
3. Growth of Privacy Laws:
   - There has been a significant increase in countries implementing comprehensive privacy laws, rising from 10% of the global population in 2020 to 82% today.
4. Challenges of AI:
   - The rapid pace of AI adoption brings new challenges related to privacy, consumer safety, and algorithmic discrimination.
   - There is a lack of organisational structures to address these complex, cross-domain issues effectively.
5. Need for Skilled Professionals:
   - The demand for AI governance professionals is critical as existing professionals are being tasked with new AI-related responsibilities.
   - There's an urgent need for upskilling within the current workforce to manage AI's multifaceted challenges.
6. Addressing Entropy:
   - The concept of entropy relates to the disorder within organisations struggling with AI policy; new energy and innovation are needed to combat this.
   - Stakeholders must introduce new frameworks and resources to ensure effective compliance with evolving AI standards.

Proposed Actions for Stakeholders:

- Upskill Workforce: Invest in training and upskilling existing professionals in AI governance and digital policy.
- Create Collaborative Frameworks: Encourage cross-departmental collaboration within organisations to handle AI and privacy-related issues effectively.
- Engage in Policy Development: Participate in discussions on AI policy to shape regulations that address the rapidly changing technological landscape.
- Focus on Diversity: Encourage a diverse range of professionals to engage with AI governance to fill the gap of expertise across different domains.

By taking these actions, stakeholders can effectively address the challenges posed by AI and ensure a structured and responsible approach to digital governance.

Isabelle Roccia

Managing Director, Europe, IAPP

I would not bore you with an inventory of everything that's going on in Brussels, but focus my remarks on some of the trends and some of the more structural elements that we see emerging right now that will likely inform the way European digital regulation, and specifically with AI, will emerge. Of course, some of that is already influenced by the geopolitics as we are all witnessing them.

Mario Draghi Report on Competitiveness

So taking my two cents with a grain of salt, I guess I want to start with a statement around the report from former Prime Minister Mario Draghi on EU competitiveness. This has been, I think, a very important milestone in the last few months and the importance of that report and its findings and its call for action on the EU side on competitiveness and the challenges to that dynamic in Europe should not be underestimated.

Simplification of Legal Frameworks

The notion of having a simplified legal framework, being able to draw more investment in Europe to support the emergence of infrastructure and skills are very much trends that we see building up in the policy agenda in Brussels. And of course, all of those are relevant when we talk about artificial intelligence.

Conversations in Brussels

So I think there's a genuine conversation happening in Brussels around that dynamic. And I think it is reflected as well, of course, by some of the political equilibrium that we observe in Member States and reflected in the European Parliament as well towards perhaps some more resonance for trends around building independence of the EU. So simplification has a lot of dynamic and political will behind it at the moment in Brussels.

Legislative Pause Does Not Mean Inactivity

I do want to nuance that as well, sort of routing it back to the conversation and the practitioners and the operationalisation aspect of what we're discussing today. And even if there's a pause on the legislative agenda in Brussels, that doesn't mean that nothing will happen. I think we're witnessing and expecting a lot of activity, be it non-legislative, regulatory action plans and so on.

The AIX (a series of proprietary Unix operating systems) was mentioned already; I think that's an example of something that will continue to live through a number of actions throughout the coming months and years. But so do things like the GDPR, which has been in force for eight years now and is still subject to much debate and discussion, and is a source of those frictions, tensions, and complications that practitioners have to navigate.

So hitting the pause button in Brussels from a legislative standpoint will not necessarily mechanically translate into that legal certainty and clarity that I think some of the tensions we're talking about might be calling for. Eddie Joe's team is doing amazing work at trying to map and quantify some of those tensions as well.

EU’s Regulatory Agenda and External Promotion

So that's one point: the fact that pause doesn't equal inactivity. The second point is really around the EU's agenda and willingness to continue to export and promote its regulatory agenda outside its borders. Given the current environment, the EU is likely to double down on its efforts to promote its regulatory model and its values model outside its own borders.

Areas to Watch in AI Regulation

I want to mention a few areas to watch that will resonate with Trevor's remarks and hopefully tie up some of the elements that our industry panel will dive a bit more into. In terms of areas to watch, I want to mention maybe just five very briefly:

1. Intersectionality and Stakeholder Mapping: This is really where the rubber meets the road in Brussels right now, particularly in terms of the compatibility, or sometimes lack thereof, of different instruments at play. A big focus is on how to create stakeholder mapping of who the regulators are going to be working on those issues, ensuring that they speak the same language, and have mechanisms for cooperation and collaboration.
2. AI Liability and GDPR: We still have question marks on specific areas that had been introduced in the previous term and have yet to be fully addressed with this new mandate, such as AI liability and a potential targeted revision of the GDPR.
3. Privacy and Security Articulation: The articulation between privacy and security is also going to be a significant focus, with relevance to AI as well.
4. Data Retention and Cybersecurity Resilience: Issues such as data retention, encryption, and cybersecurity resilience are coming back to the forefront in the Brussels agenda, including the security of infrastructures like undersea cables.
5. Sovereignty and Industrial Policy: The sovereignty element will be increasingly important through industrial policy and public procurement, influencing not only the legislative agenda in Brussels but also the positioning across various industrial policy dynamics emerging in this context.

Data Transfers as an Ongoing Issue

Lastly, data transfers will likely pop up again on the agenda very soon, with considerations playing out in Brussels regarding instruments already in place with various jurisdictions. These elements will have concrete implications for practitioners and will also inform how Europe continues to advance its artificial intelligence agenda. This, in turn, will influence governance and the operationalisation aspects of these issues down the line.

Conclusion

So, thank you very much for your time. Those are the key trends and areas to watch regarding European digital regulation, especially in the context of AI. It’s essential for all stakeholders to stay informed and engaged with these developments as they unfold.

Summary of Isabelle Roccia's Key Points and Actions for Stakeholders

1. Importance of the Mario Draghi Report:
   - Recognises the report as a significant milestone for EU competitiveness, highlighting the call for a simplified legal framework to attract investment and support infrastructure and skills development.
2. Active Conversations in Brussels:
   - Notes the genuine discussions regarding the simplification of regulations in light of geopolitical factors and the political equilibrium within Member States and the EU Parliament. Encourages stakeholders to engage in these dialogues.
3. Legislative Pause Does Not Imply Inactivity:
   - Clarifies that even with a pause in the legislative agenda, there will be ongoing non-legislative activities such as regulatory action plans. Stakeholders should prepare for continued developments in the policy landscape.
4. Need for Stakeholder Mapping:
   - Highlights the focus on mapping regulators and ensuring collaboration among various stakeholders. Advocates for the establishment of clear communication mechanisms among regulatory bodies.
5. Regulatory Areas to Monitor:
   - Identifies five priority areas for stakeholders to watch:
     - Interplay of Regulatory Instruments: Understanding the compatibility of different regulatory frameworks.
     - AI Liability and GDPR Revisions: Watch for discussions around AI liability and potential revisions to GDPR.
     - Privacy and Security Articulation: Focus on how privacy and security regulations are integrated, particularly concerning AI applications.
     - Data Retention and Cybersecurity: Pay attention to emerging discussions on data retention policies and cybersecurity measures, including infrastructure security.
     - Sovereignty and Industrial Policy: Recognise the growing emphasis on sovereignty within industrial policy and public procurement that will shape the regulatory landscape.
6. Anticipation of Data Transfer Issues:
   - Foresees renewed focus on data transfer regulations, urging stakeholders to stay updated on developments and implications for cross-border data flows.

Actions for Stakeholders:

- Engagement: Actively participate in regulatory discussions and provide input to shape effective and practical regulatory frameworks.
- Collaboration: Foster cooperation and communication among industry peers, regulators, and policymakers to ensure cohesive approaches to regulatory compliance.
- Monitoring Developments: Stay informed about legislative changes, regulatory guidance, and evolving discussions in the EU regarding AI and digital regulations.
- Preparation for Operational Changes: Anticipate how new regulations will impact business operations and governance structures to maintain compliance and leverage opportunities.

By focusing on these points and taking the proposed actions, stakeholders can better navigate the complexities of European digital regulation and contribute to shaping a forward-looking AI landscape.

Jeanine Mckelvey

General Counsel
Group Data Privacy & Ethics Officer
BT

My name is Jeanine Mckelvey and I am from BT. I think my title is a good reflection of how BT is responding to all of these evolving laws: the General Counsel for Data, AI, and Security. Now, that's quite a new concept in the UK to have a General Counsel that is specifically focused on data, AI, and security. It’s a recognition by BT that we are sitting on a tremendous amount of data, which is very important to us and to the country. AI is very important to us, and security is very important to us, and there are a number of laws that intersect in that space.

Need for a Dedicated Department

If you think about critical infrastructure legislation and online harms that Joe just mentioned, a lot of the emerging AI laws that BT is facing off against in 180 different countries, and a lot of the emerging data laws, there was a recognition that there needed to be a department and a function focused on all of these emerging laws because we couldn’t just look at personal data and think we’ve solved the problem. We actually needed to look at all data and we had to look at it in certain critical spaces.

Role as Group Data Protection and Ethics Officer

I should also say I am the Group Data Protection and Ethics Officer, but for me, that is a smaller title now because that pertains to personal data, whereas my world and my responsibility is for all of these data laws because they are all critical to our business. I need to be thinking, and my team needs to be thinking, about how we build the right standards, controls, policies, and governance to ensure that we navigate all of these emerging laws in different countries.

Team Composition for Compliance

Now, my team and the makeup of that team is a response to just how we get this right. My team is not comprised just of lawyers; I probably have more compliance and assurance people in my team now than I do lawyers. They are a mixture of risk, governance, security, and technology folk who work very closely with the lawyers to ensure that we can deliver against all of these emerging requirements.

Building Trust with Customers

For those of you who are BT customers or not, one of our purposes is to be the most trusted connector of people, devices, and machines, and the keyword there is trust. Because if people don't trust us with their data, they're not going to give it to us. If we don't get the data, we can't do great things with AI and we can't spur innovation. So getting it right with data and ensuring we have the right guardrails and frameworks to gain our customers' trust is key to what we do.

Approach to AI and GDPR Compliance

When it comes to AI, the way we are approaching this is that we are building on all the good things we did for GDPR. For GDPR, we built things like privacy impact assessments, which have evolved now to be an impact assessment that takes account of more than just the GDPR questions we used to ask. We now ask human rights questions and ethics questions. We are looking at the guidance coming out of the ICO and the CMA in all of these spaces and incorporating those questions for the business to answer.

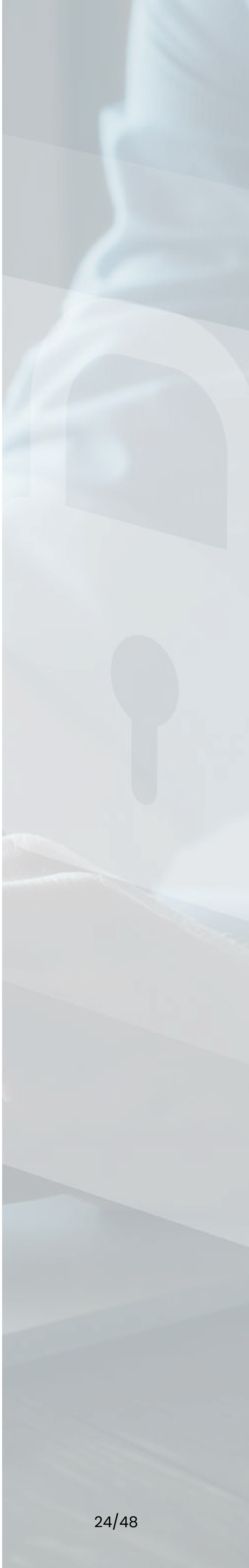
Collaboration Across Disciplines

We are building on things like the records of processing activity. We need an inventory to wrap our arms around AI. We're considering where we build, develop, and use AI and making sure that whatever we have in place for all those areas originally created for GDPR are now scaled up. We're making sure we're upskilling people and training them. We are working far more closely with our data engineers, data architects, and data scientists.

It requires skills and collaboration; it requires people to be able to speak each other's languages. Lawyers can interpret the law, but that doesn't necessarily mean they can help the engineers translate that into operational requirements and deliverables.

Educational Improvements for Future Professionals

I sit on an Advisory Board for Exeter University, and I frequently emphasise that data protection, data ethics, and trust need to be taught not just in the law faculty but also in the engineering and business faculties. We need graduates who can at least identify issues and employ the right expertise to tackle those challenges.



Challenges of Navigating Multiple Laws

One of our challenges from an industry perspective is that we want to do the right thing, but there are numerous laws to navigate, with emerging laws in different jurisdictions. We can't just comply with UK laws if we want to sell goods in other jurisdictions, which means the AI and evolving data laws in those countries will impact us, even if we don't have head offices there.

Importance of Common Principles and Standards

The more we can establish common principles and standards, the less money and complex red tape businesses will have to face. When I look at 180 countries and all of this legislation, I cannot build something that complies exactly with everything. So, I look for the common principles that run through these pieces of legislation, aiming to cover at least 80% of those principles. Then, I also look for new answers that are particularly relevant to our products and services.

Utilising Standards for Compliance

I do look at standards like the NIST standard and ISO standards. By the way, the ICO's guidance is excellent in these areas. I've actually heard people in other countries refer to how great the ICO's work is in this space. The more we can try to find a way that doesn't require businesses to jump through multiple hoops if they want to trade or sell their products in various territories, the better.
Lessons from the EU AI Act

I also look at the EU AI Act because it helped me build a framework—what I call a scarecrow. It was helpful to see what the EU thinks constitutes high-risk, medium-risk, and low-risk AI applications. Here, we have a principles-based approach that fosters innovation, but we also need to provide businesses with some idea of what "good" looks like and what that scarecrow entails.

Conclusion and Call to Action

By looking at the standards that organisations like ISO, NIST, and the various laws are proposing, we can begin to hang the clothes on that scarecrow. I will leave you with this: we need skilled people. From grassroots in universities, we need to start teaching these concepts throughout educational programs. We also need to aim for innovation, but to do it safely. This will help our businesses determine the necessary guardrails, and wherever possible, we should work towards harmonising with other jurisdictions.

Summary of Jeanine Mckelvey’s Key Points and Actions for Stakeholders

1. Role and Focus at BT:
    - Discusses her dual role at BT as the General Counsel for Data, AI, and Security, alongside her responsibilities as the Group Data Protection and Ethics Officer.
    - Highlights the significance of having a dedicated department to address the complexities surrounding data, AI, and security laws due to their intersection and importance to the business.
2. Building Trust with Customers:
    - Emphasises the importance of trust in customer relationships regarding data sharing, noting that customer trust is essential for data generation and innovation in AI.
3. Adapting to Evolving Laws:
    - Talks about BT's proactive approach in navigating numerous emerging laws and regulatory frameworks across 180 countries, reinforcing the need to consider global compliance rather than just focusing on UK laws.
4. Team Composition and Collaboration:
    - Describes the diverse composition of her team, which includes compliance, assurance, risk, governance, and technology professionals, working collaboratively with lawyers to meet emerging legal requirements.
5. Focus on Education and Skills Development:
    - Stresses the necessity for teaching data protection, ethics, and trust not just in law faculties but also in engineering and business programs, to prepare future professionals who can identify and address relevant issues.
6. Establishing Common Principles:
    - Encourages the search for common principles across different jurisdictions' laws to simplify compliance for businesses and reduce regulatory burdens.
7. Utilising Standards for Guidance:
    - Highlights the importance of established standards (e.g., NIST and ISO) and guidance (e.g., ICO) in shaping compliant practices and understanding the regulatory landscape.
8. Framework Development through the EU AI Act:
    - Utilises insights from the EU AI Act to create a “scarecrow” framework that helps define risk levels (high, medium, low) associated with AI applications, providing businesses with a clearer understanding of regulatory expectations.

Actions for Stakeholders:

- Embrace Collaborative Approaches: Engage diverse teams that include legal experts, compliance officers, and technology specialists to address emerging regulatory requirements effectively.
- Foster Trust: Prioritise building customer trust in data handling to facilitate innovation and data sharing.
- Advocate for Educational Reforms: Work with educational institutions to incorporate data protection, ethics, and AI-related topics across various curricula.
- Seek Harmonisation of Standards: Support efforts to establish common regulatory principles that ease compliance challenges for businesses operating in multiple jurisdictions.
- Utilise Available Resources: Leverage existing standards and regulatory guidance to inform practices and establish robust compliance frameworks.

By implementing these points and actions, stakeholders can better navigate the evolving landscape of data and AI regulations while fostering innovation and maintaining ethical standards.

Lara Liss

Chief Privacy and Data Trust Officer, GE HealthCare

I'm Lara Liss, Chief Privacy and Data Trust Officer for GE Healthcare, where I lead our global privacy programme and co-lead our responsible AI programme together with our Chief AI Officer. I appreciate the opportunity to speak to this AIA PG evidence meeting on the future of digital governance, and I want to thank the co-chairs, Lord Clement Jones and Alison Gardner, MP, as well as the other members of the AIA PG for bringing together these stakeholders to discuss this highly relevant topic that, if effectively addressed, has the potential—through increased innovation and AI—to improve the quality of care for our patients as well as reduce the cognitive stress for our providers.

The Role of AI Governance Professionals

We are at a turning point where AI governance professionals play a critical role in navigating digital entropy. The fragmentation of policies, frameworks, and accountability across digital systems, without clear professionalised oversight, means that AI risks becoming an uncoordinated force, amplifying regulatory conflicts and ethical dilemmas. This is why today's discussion is so vital.
Benefits of AI in Healthcare

How can policymakers, regulators, and industry leaders coordinate digital law and governance to foster accountability and responsible AI? AI has already demonstrated significant benefits in healthcare, improving diagnostic accuracy, streamlining workflows, and enhancing patient outcomes. By leveraging AI, healthcare providers can automate routine tasks, reduce cognitive stress for clinicians, and enable more precise and personalised treatment plans.

Examples of Innovation in Healthcare

To give you a better understanding of what this innovation looks like in the healthcare space, I want to highlight three examples of our technology that is in use today and how it can help improve care.

1. Mobile X-Ray Devices: The first example is the use of AI on mobile X-ray devices to help detect critical conditions such as pneumothorax, which is a collapsed lung, so that the care team can act quickly.
2. MRI Scanners: The second example is the use of AI in MRI scanners to reduce scan times, which improves patient experience while also enhancing image quality. If you've ever been in an MRI scanner or had a loved one who's been in an MRI scanner, you know how important that patient experience is.
3. Ultrasound AI Scan Guidance: The third example of innovation in the healthcare space is the use of ultrasound AI scan guidance. Ultrasound is incredibly operator-dependent, and the healthcare professional performing the ultrasound exam needs to have a certain level of training as well as experience to capture high-quality medical images. Our AI scan guidance helps less experienced users capture diagnostic, usable images too. This is especially helpful given the shortage of healthcare workers.

Importance of Risk Management in AI

Before diving into the specifics of risk management, it's important to recognise that AI systems operate in complex and evolving environments. Their effectiveness depends not only on the quality of their training data but also on the governance mechanisms that guide their deployment. Without a structured approach, AI can introduce unintended biases, inconsistencies, and security vulnerabilities.

Here are a few considerations based on my work in the healthcare industry:

1. Integration of Risk Management Frameworks: Risk management frameworks must be built into AI systems from the start and not as an afterthought.
2. Human Oversight: Human oversight remains essential to prevent hallucinations, misrepresentation, and unintended consequences.
3. Change Control and Life Cycle Monitoring: Change control and life cycle monitoring ensure continuous oversight and adaptation to evolving risks. AI professionals must be at the centre of these governance efforts.

Professionalisation of AI Governance

The IAPP emphasises that professionalisation is not just about compliance but about ensuring AI works within a structured, accountable ecosystem. This is crucial as digital law continues to evolve across different jurisdictions, creating regulatory tensions.

Key Recommendations Moving Forward

So, where do we go from here? I'll leave you with four key recommendations:

1. Codify the Role of AI Governance Professionals: AI oversight must be recognised as a specialised discipline, with clear training, certifications, and ethical guidelines. I say there are three key skills that we have as AI governance professionals: we are navigators, we are translators, and we are diplomats, and that needs to be recognised.
2. Adopt Structured Adaptive Governance Frameworks: Adopt structured adaptive governance frameworks that are industry-specific where appropriate. As a medical device company, we operate in a highly regulated space under the close watch and guidance of medical device regulators around the world, including the Medicines and Healthcare Products Regulatory Agency (MHRA) here in the UK. The expertise of these regulators about our industry is immense.
3. Foster Cross-Border Coordination: As AI regulations emerge, harmonising global digital policies will be essential to reducing conflicts and ensuring seamless compliance.
4. Strike the Right Balance in Regulation: Strike the right balance in regulation—one that protects patient safety, focuses on high-risk areas, but still allows innovation to move at speed. I keep thinking about how these new technologies could transform outcomes, helping people live longer, healthier lives. The sooner we can bring these tools to patients safely, the better, especially in areas like cancer detection and treatment.

Shift from Treatment to Prevention

And it's not just about treating illness; it's about shifting from sick care to prevention and early detection. With structured professionalisation, AI could become a force for clarity, accountability, and responsibility, not entropy.

Summary of Lara Liss's Key Points and Actions for Stakeholders

1. Position and Responsibilities:
    - Lara Liss is the Chief Privacy and Data Trust Officer at GE Healthcare and co-leads the company's responsible AI programme.
    - Highlights the importance of addressing AI governance effectively to enhance patient care and reduce the cognitive stress on healthcare providers.
2. Critical Role of AI Governance Professionals:
    - Emphasises the importance of AI governance professionals in navigating digital entropy, which encompasses the fragmentation of policies and accountability across digital systems.
    - Stresses the need for clear professional oversight to prevent AI from becoming an uncoordinated force that amplifies regulatory conflicts and ethical dilemmas.
3. Significant Benefits of AI in Healthcare:
    - Discusses how AI has improved diagnostic accuracy, streamlined workflows, and enhanced patient outcomes.
    - Provides examples of AI applications:
        - Mobile X-ray Devices: Helping detect critical conditions quickly.
        - MRI Scanners: Reducing scan times for a better patient experience.
        - Ultrasound AI Guidance: Assisting less experienced users in capturing diagnostic images.
4. Importance of Risk Management in AI:
    - States that AI systems require robust risk management frameworks from the outset.
    - Highlights the necessity of human oversight to prevent unintended consequences and emphasises the need for change control and life cycle monitoring to address evolving risks.
5. Professionalisation of AI Governance:
    - Argues that the professionalisation of AI governance is essential for ensuring a structured and accountable ecosystem that aligns with evolving digital laws across jurisdictions.
    - Recommends that AI oversight should be recognised as a specialised discipline with defined training, certification, and ethical guidelines.

Recommendations for Stakeholders:

- Codification of AI Governance Role: Establish clear roles and responsibilities for AI governance professionals.
- Adoption of Structured Governance Frameworks: Implement industry-specific governance frameworks to navigate regulatory environments effectively.
- Fostering Cross-Border Coordination: Encourage harmonisation of global digital policies to minimise conflicts and enhance compliance.
- Balancing Regulation and Innovation: Ensure regulations adequately protect patient safety while allowing for rapid innovation in healthcare.

By focusing on these points and implementing the suggested actions, stakeholders can foster a responsible AI environment that enhances healthcare delivery, promotes trust, and drives innovation in patient care.

Simon McDougall

Chief Strategist, Privacy and AI,
ZoomInfo

My job title nowadays is Chief Strategist, Privacy and AI. For my sins, in a previous life, I was also the Deputy Commissioner at the Information Commissioner's Office, a regulator here in the UK.

About ZoomInfo

ZoomInfo is a business-to-business data broker. It's nothing to do with the video conferencing company. It’s one of those companies that works mainly behind the scenes in the sales and marketing sector. It's large enough—about 1.2 billion in revenues and listed on the NASDAQ—but most people in the UK are not too familiar with it. We process about 1.6 billion data points a day. But we are boring. We are a boring B2B company.

Data and Transparency Practices

We don’t have children’s data, we don’t have geolocation data, and we don’t do deep profiling and know whose dog likes to eat this dog food or that dog food. We are a B2B data broker with very limited data sets on the organisations and the people we work with—about 250 million people in our database and 100 million companies.
So you could say, well, why do we care about this? It’s not getting a lot of the hot topics you might see in the EAI Act. The hot topics that Lara and Jeanine are dealing with are not necessarily the kind of things we deal with.

Corporate Interests in AI Governance

While, on one level, we want to do the right thing, and I would have joined in from the regulator point of view, if we didn’t believe that, on another level, it is cold, hard capitalism. Our corporate customers care about AI governance; they've always cared to some extent about privacy and data provenance because they want to know how we got hold of the data and how we're using it.

At that level, we’re no different from a supermarket having to know where its chicken came from or a jeweller selling engagement rings needing to know where the diamonds came from. There have always been questions around data provenance and transparency in the marketplace, but what I think has changed with AI is the understanding of how valuable data is.

Shifts in Data Value Due to AI

It’s changed because people understand the scale of data needed to be a cutting-edge company, and it’s scaled because we can do more inferences and derive more insights from the data.

For ZoomInfo, as a company, one of the key things is that, as we work with our corporate customers, which include most of the largest companies in the world, before we effectively sold them data, we were effectively a data broker. Now, the value is much more than just commingling the data; it’s around us taking data from our customers, working with them, and giving them better data back. We’re providing them data to use because that’s how this new world of AI generates value.

Building Trust Across Supply Chains

You can’t do that unless you have a deeply trusting relationship between different players in the supply chain. We do want to do the right thing, but as we talk to our corporate customers, they come to us with questions about how we handle data, how we manage AI, and if they share their data, how they can be assured it isn’t going to be commingled elsewhere or shared elsewhere.

Are we using their data to train our models? How does that work? What we have seen since the advent of ChatGPT-3.5 is an increasing level of sophistication in the questions we receive. Without being disparaging, we had conversations early on that were much more about wanting a personalised service without being willing to let us do anything with their data.

Evolving Conversations on Data Use

Now, we are having quite sophisticated dialogues about how that works. We're moving to a world where supply chains are far more iterative and interactive, and AI governance is a way to establish trust across those supply chains.

Practical Points for Implementation

I'll finish off with a few practical points to paint a picture of how we've done this. As with everybody else, while we've used machine learning for many years, we were caught out by Chapter 53.5 and this wave of LLMs, just as everybody was.

We had to spend a lot of time with my compliance teams and the business to work on real messaging and to build governance as we went. Now we're in a stage where we have third-party certifications to explain to our customers, in shorthand, why we are responsible and what we do. We use AI to help our salespeople explain why we're good at AI.

Incorporating AI in Customer Interactions

So, they have live chatbots that surface the right documentation and answer the questions. It does become a little bit circular in that respect.

Future Expectations and Real-World Consequences

In the future, I think this is only going to become more pressing as we enter this wave of agentic AI, where there are real-world consequences to what we're doing. People expect to have more decision-making occurring within this rather than just data analysis. I think the stakes are being raised for everybody.

Even regardless of how much heavy regulation we face, and in terms of the regulatory tides going in or out, we will have incidents. Things will happen in the market, and corporate customers will expect us to be good corporate citizens.

Conclusion on AI Governance as a Commercial Imperative

So for us at ZoomInfo, and I think for all private sector organisations, good AI governance will continue to be a commercial imperative as well as a regulatory imperative.

Summary of Simon McDougall’s Key Points and Actions for Stakeholders

1. Current Role and Background:
    - Simon McDougall is the Chief Strategist, Privacy and AI at ZoomInfo and formerly the Deputy Commissioner at the Information Commissioner's Office in the UK.
2. Overview of ZoomInfo:
    - ZoomInfo is a business-to-business data broker, processing about 1.6 billion data points daily, with a focus on privacy, transparency, and data provenance.
    - Unlike companies handling sensitive personal data, ZoomInfo deals with data relevant to business organizations and professionals, including limited data sets on 250 million individuals and 100 million companies.
3. Corporate Interest in AI Governance:
    - Highlights that corporate customers are increasingly interested in AI governance, privacy, and data management due to the commercial implications of data use and provenance.
    - Compares the need for transparency in data practices to established industries, such as the origins of food and jewellery.
4. Changing Value of Data:
    - Emphasises that the understanding of data's value has evolved, as companies recognise the scale of data required to remain competitive and the importance of inference derived from data.
    - ZoomInfo's value has shifted from merely selling data to building trusted relationships with clients to provide enhanced data for decision-making.
5. Building Trust in Data Practices:
    - Focuses on the importance of trust between data providers and customers, particularly in ensuring that data is not improperly shared or commingled.
6. Evolving Conversations on Data Use:
    - Notes a shift in customer conversations from simplistic expectations about data usage to more sophisticated inquiries regarding data management and AI application.
7. Practical Implementation of Governance:
    - Discusses the journey to build governance frameworks in response to rapid developments in AI and machine learning, especially after significant advancements like ChatGPT-3.5.
    - Mentions the importance of compliance teams and messaging to ensure clarity in governance communications.
8. Use of AI in Customer Interaction:
    - Describes the implementation of AI, such as live chatbots, to assist in providing information and addressing customer inquiries about data practices efficiently.
9. Future Challenges and Expectations:
    - Warns that as AI evolves, the stakes will rise in terms of real-world consequences from AI applications, and businesses will be expected to act as responsible corporate citizens.
    - Articulates that incidents will occur, regardless of regulatory pressures, highlighting the need for businesses to uphold good AI governance.
10. Commercial and Regulatory Imperative:
    - Concludes that effective AI governance is not just a regulatory requirement but also a commercial imperative for businesses in the private sector.

Actions for Stakeholders:

- Enhance Trust: Foster transparent data practices and clear communication about data use to build trust with corporate customers.
- Emphasise Governance: Implement robust governance frameworks from the outset of AI projects, rather than as an afterthought.
- Engage in Sophisticated Conversations: Be prepared for complex discussions around data management and use as clients become more knowledgeable.
- Utilise Technology Effectively: Leverage AI and chatbots for efficient customer engagement and to maintain clarity in governance discussions.
- Focus on Responsibility: Ensure that organisations are prepared for the real-world implications of AI usage and uphold responsibilities as good corporate citizens.

By addressing these points, stakeholders can navigate the evolving landscape of AI governance effectively while meeting both regulatory and commercial expectations.

BIOs of Evidence Givers

Trevor Hughes
CEO & President
IAPP

J. Trevor Hughes is the president and CEO of the IAPP, the professional home for privacy, AI governance and digital responsibility globally. With over 80,000 members in more than 150 countries, the IAPP provides training, certification, publications, research, events and networking opportunities to respond to growing need for professionals to manage the intersections of data, technology and humanity.

A native of Canada, Trevor previously served as the executive director of the Network Advertising Initiative and the Email Sender and Provider Coalition.

Trevor is widely recognized as a leading digital policy expert on the global stage. He is a sought-after speaker, appearing at SXSW, RSA Conference, TEDx, the Global Privacy Assembly and more. Recent speaking engagements have included ICA Live: Africa, World Bank Group Data Privacy Day, the FIFA Global Compliance Summit and the Mobile World Congress Ministerial Programme. He has lectured extensively around the world, including at Harvard, MIT, London School of Economics, Trinity College Dublin, University of Texas at Austin, and Northeastern University Law School.

Trevor has contributed to media outlets such as The New York Times, TechCrunch and Wired and has testified on issues of privacy, surveillance and privacy-sensitive technologies before U.S. Congress, the U.S. Federal Trade Commission, British Parliament and more.

He received his bachelor's degree from the University of Massachusetts Amherst and his Juris Doctor degree from the University of Maine School of Law, where he is an adjunct professor.

Joe Jones
Director of Research & Insights
IAPP

Joe provides strategic direction and leadership for the development of practical content for privacy, AI governance, and digital responsibility professionals on law, policy, technology, and management issues. This work includes engaging with privacy leaders from industry, government, academia and civil society as he keeps IAPP members informed on data protection developments around the world.

Previously, Joe served as a senior civil servant with the UK Government, leading teams responsible for the policy design and delivery on international data protection and digital governance matters. This included work on data adequacy with the EU, United States, and other key partners, which involved Joe leading dozens of diplomatic delegations. Prior to working for the UK Government, Joe worked as a lawyer with Covington & Burling LLP, advising companies on tech law and policy matters.

Joe has been globally recognized as a leader in privacy law and policy. In 2022, Politico named him as the fourth most influential 'rulemaker' in Europe as well as the Digital policy 'Wonk of the week' in September of 2021.

Isabelle Roccia
Managing Director, Europe
IAPP

As Managing Director, Europe, Roccia leads the IAPP's growing Brussels office and engages with senior industry leaders, policymakers, regulators and civil society, keeping IAPP members informed and apprised of local developments. She serves as the public voice for the IAPP across Europe and provides strategic guidance on European engagement and market expansion.

Prior to joining the IAPP, Roccia served as Director of Policy, EMEA of BSA | The Software Alliance in Brussels, Belgium. In this role, she developed and advanced policy positions on a range of key issues to the global software industry, with a focus on data privacy, international data flows, cybersecurity, digital trade and digital transformation. She is a recognized contributor to policymaking on these issues on national, European and multilateral levels. Prior to that, Roccia was the Senior Policy Advisor at the U.S. Mission to the EU in Brussels.

Lara Liss
Chief Privacy & Data Trust
GE HealthCare

Lara Liss is chief privacy and data trust officer at GE HealthCare. She is an experienced in-house attorney and compliance professional with expertise in privacy, responsible AI, data security and health care who has led global privacy compliance and legal teams at two Fortune 100 healthcare companies, a USD19 billion medical device and technology company and a domestic health care system. She founded and co-led the Responsible AI program at Walgreens Boots Alliance and now at GE HealthCare. Her practice includes new and emerging areas of digital governance and privacy law such responsible AI, biometrics, clinical trials, pharmacogenomics and developing technologies such as drones for retail.

Lara has a J.D. and a Master of Public Policy degree from the University of Michigan, a B.A. in American Studies from Northwestern University and is a Certified Information Privacy Professional-US. This fall, she will complete her Executive MBA at Northwestern University's Kellogg School of Management.

Janine McKelvey
General Counsel
Group Data Protection & Ethics Officer
BT Group

Janine leads a multidisciplinary team of data lawyers, compliance, and assurance professionals for BT's business units in the UK and internationally across 180 jurisdictions. Her team are responsible for advisory and assurance obligations relating to existing and emerging data laws, including AI, data ethics, data governance, privacy and security.

Prior to joining BT, Janine was an SVP of Legal and Business Affairs at Warner Bros. for many years and in private practice with Pinsent Masons (UK) and Bowmans (RSA).

Janine is a dual qualified English and South African lawyer and an advocate for responsible technology.

Simon McDougall
Chief Strategist, Privacy and AI
Zoominfo

Simon McDougall is the Chief Strategist, Privacy and AI, of Zoominfo, a leading provider of business information and intelligence.

He is responsible for ensuring that Zoominfo's products and services comply with applicable laws and regulations, as well as industry best practices. He has over 15 years of experience in the field of data privacy and compliance, having previously worked as the Executive Director for Technology Policy and Innovation at the UK Information Commissioner's Office (ICO) and as a Managing Director at Promontory Financial Group.

ABOUT

iapp

International Association of Privacy Professionals

The IAPP is a non-profit, policy-neutral organisation with a mission to define, promote and improve the professions of privacy, AI governance, and digital responsibility globally.

IAPP’s policy-neutral posture is rooted in a simple idea. No matter how rules and best practices evolve, a community of capable and connected professionals is needed to design and implement responsible digital governance within organizations of all types.

It provides members with the tools, resources, research, training, credentials, and networking needed to thrive in today's digital economy.

Since its founding in 2000, the IAPP’s membership has grown to over 85,000 across 150 countries, and it has issued over 45,000 professional certifications around the world.

ABOUT APPG AI

All Party Parliamentary Group on
Artificial Intelligence

ABOUT:

APPGs are informal cross-party groups in the UK Parliament. They are run by and for Members of the Commons and Lords. The All-Party Parliamentary Group on Artificial Intelligence (APPG AI) functions as the permanent, authoritative voice within the UK Parliament (House of Commons and House of Lords) on all AI-related matters, and it has also become a recognisable forum in the AI policy ecosystem both in the UK and internationally.

Parliamentary APPG AI Members: House of Commons

- Allison Gardner MP Labour (APPG AI Co-Chair)
- Alison GRIFFITHS MP Conservative
- Andrew Pakes MP Labour
- Bell Ribeiro-Addy MP Labour
- Chris Kane MP Labour
- Daniel Aldridge MP Labour
- Danny Chambers MP Liberal Democrat
- Dave Robertson MP Labour
- David Reed MP Conservative
- Dawn Butler MP Labour (APPG AI Vice-Chair)
- Esther McVey MP Conservative
- George Freeman MP Conservative
- Gordon McKee MP Labour
- Graham Leadbitter MP SNP
- Liam Byrne MP Labour
- Mike Martin MP Liberal Democrat
- Martin Wrigley MP Liberal Democrat
- Maureen Burke MP Labour
- Peter Fortune MP Conservative
- Samantha Niblett MP Labour
- Sarah Edwards MP Labour
- Tom Collins MP Labour
- Tom Gorden MP Liberal Democrat
- Tony Vaughan MP Labour
- Sir Mark Hendrick MP Labour
- Zöe Franklin MP Liberal Democrat
- Dr Zubir Ahmed Labour

Parliamentary APPG AI Members: House of Lords

- Lord Clement-Jones (Tim Clement-Jones) Liberal Democrat (APPG AI Co-Chair)
- Viscount Camrose (Jonathan Camrose) Conservative
- Viscount Colville Of Culross (Charles Mark Townshend Colville) Crossbench
- Lord Craig of Radley (David Brownrigg Craig) Crossbench
- Lord Cromwell (Godfrey Cromwell) Crossbench
- The Earl of Erroll (Merlin Hay) Crossbench
- Lord Fairfax of Cameron (Nicholas Fairfax) Conservative
- Lord Freyberg (Valerian Bernard Freyberg) Crossbench
- Lord Strathcarron (Ian David Patrick Macpherson) Conservative
- Lord Janvrin (Robin Berry Janvrin) Crossbench
- Baroness Kramer (Susan Veronica Kramer) Liberal Democrat
- Baroness McGregor-Smith (Ruby McGregor-Smith) Non-affiliated
- Lord Ranger of Northwood (Kulveer Ranger) Conservative (APPG AI Vice-Chair)
- The Lord Bishop of Oxford Stephen Croft Bishops
- Viscount Stansgate (Stephen Stansgate) Labour
- Professor Lord Tarassenko (Lionel Tarassenko) Crossbench
- Lord Taylor of Warwick (John David Beckett Taylor) Non-affiliated (APPG AI honorary Vice-Chair)
- Baroness Uddin (Manzila Pola Uddin) Non-affiliated

aippg appg

All Party Parliamentary Group on
Artificial Intelligence

THANK YOU TO OUR SUPPORTORS

Helping Us Raise Our Ambition for What Can Be Achieved

Meet Ami Love Ami

Automated Analytics

bsi.

Brunel University London

BT Group

Capgemini

Centre for the Governance of AI

CMS law·tax·future

cognizant

Deloitte.

duolingo

EY

FAVOM

GenAirate TECHNOLOGIES

IFS

UKRI Innovate UK

Meta

onfido

Osborne Clarke

Queen Mary University of London

Santander

UNIVERSITY OF SURREY

UPTITUDE

WINDWORKX

ACCESS APPG AI RESOURCES, EVENTS AND FULL PROGRAMME

Pavilion proudly hosts the All-Party Parliamentary Group on Artificial Intelligence (APPG AI), providing a centralised hub for all its resources, including publications, event registrations, and more.

Annual Programme

At least 6 Round Table Evidence Sessions.
4 Advisory Board Meetings.
Special Policy Briefings.

Networking

All events are held in the UK Parliament and chaired by the APPG AI Co-Chairs and the Parliamentarians.

Resources

Reports, transcripts, videos, and photo albums.

Download your Pavilion App Now!

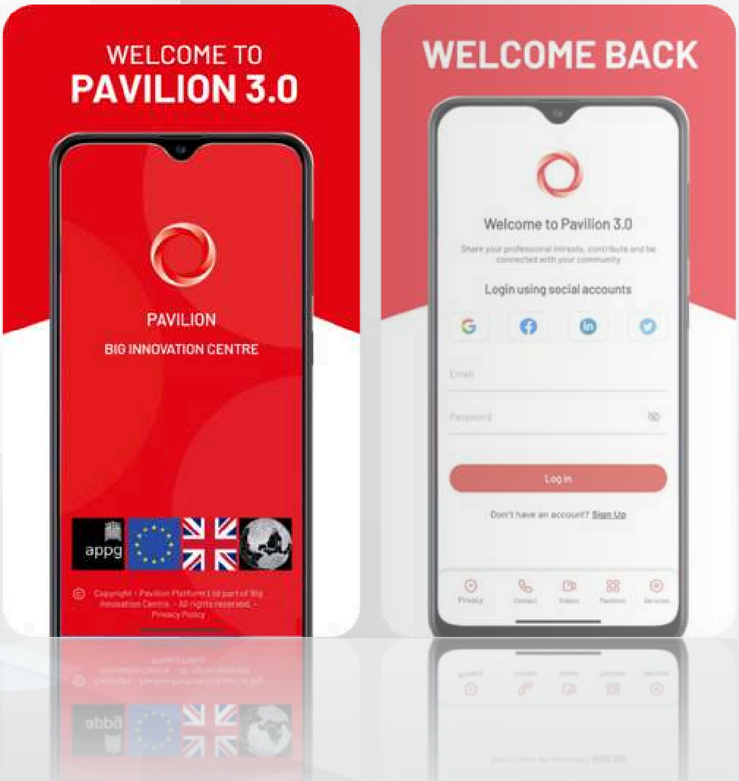
Go to APPG AI Pavilion and click on what you are looking for.

From your computer:

Pavilion on PC website: https://bicpavilion.com/

From your mobile:

Pavilion on App Store https://apple.co/4dCawaW
Pavilion on Google Play https://bit.ly/44Da6N3

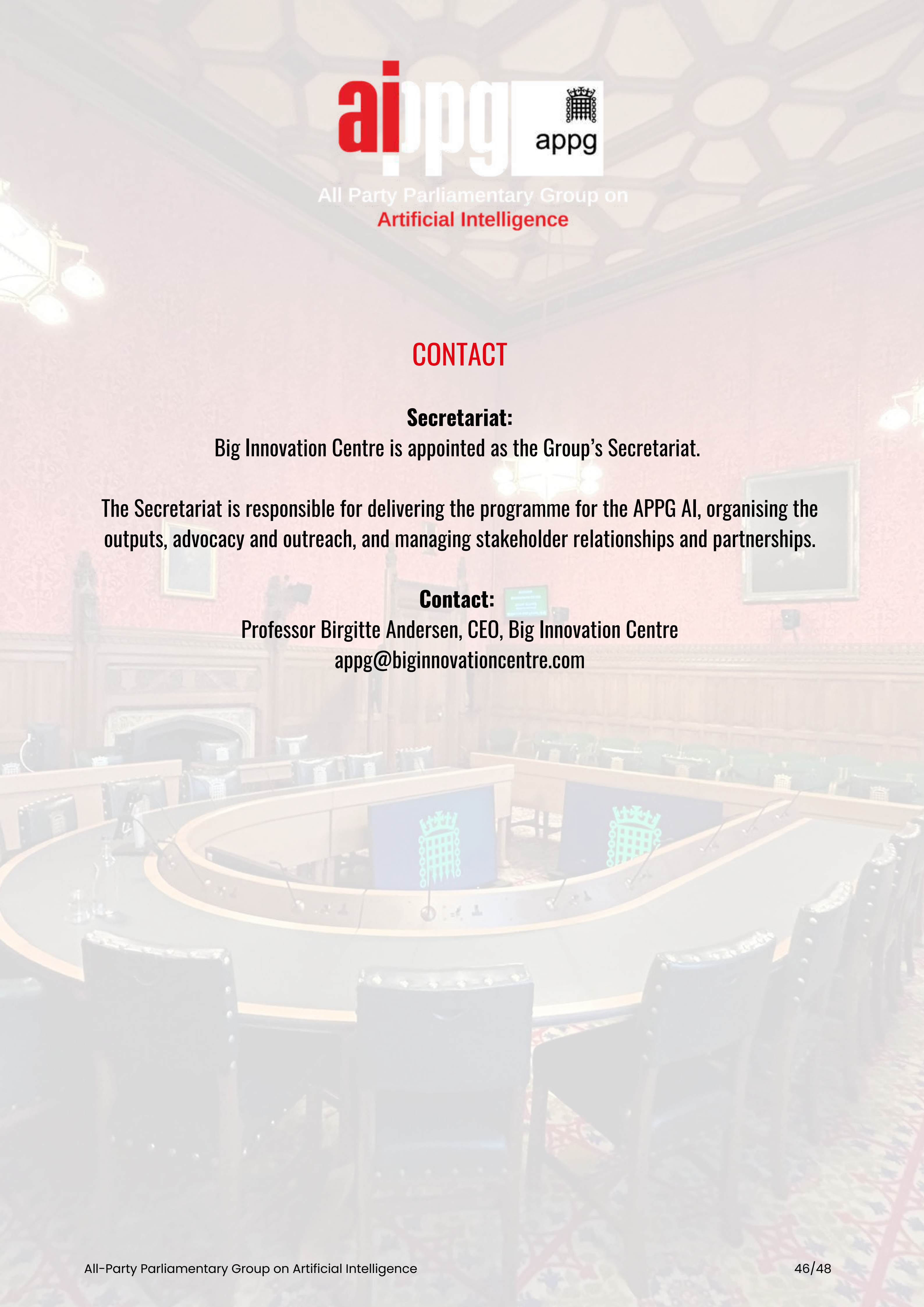


Please use the same username and password across all web and mobile app devices, avoiding the hassle of multiple accounts.
Click below:

visit our website bicpavilion.com

Download on the App Store

GET IT ON Google Play



All Party Parliamentary Group on
Artificial Intelligence

CONTACT

Secretariat:
Big Innovation Centre is appointed as the Group’s Secretariat.

The Secretariat is responsible for delivering the programme for the APPG AI, organising the outputs, advocacy and outreach, and managing stakeholder relationships and partnerships.

Contact:
Professor Birgitte Andersen, CEO, Big Innovation Centre
appg@biginnovationcentre.com

Above (from left to right): **Janine McKelvey, General Counsel** (Group Data Privacy & Ethics Officer at BT), **Simon McDougall** (Chief Strategist, Privacy and AI, at ZoomInfo), **Lara Liss** (Chief Privacy and Data Trust Officer GE HealthCare), **Joe Jones** (Director of Research & Insights of the IAPP), **Isabelle Roccia** (Managing Director, Europe, IAPP), **Lord Clement-Jones CBE** (APPG AI Co-Chair), **Trevor Hughes** (CEO & President, IAPP), **Allison Gardner MP** (APPG AI Co-Chair), **Professor Birgitte Andersen** (CEO Big Innovation Centre and APPG AI Secretariat), **Lord Holmes MBE** (House of Lords), **The Earl of Erroll** (House of Lords), **Lord Taylor of Warwick**.

All-Party Parliamentary Group on
Artificial Intelligence
appg@biginnovationcentre.com

SECRETARIAT

Big Innovation Centre is appointed by the UK Parliament as the Group's Secretariat.