All-Party Parliamentary Group on Artificial Intelligence

How can Privacy Power the AI Revolution?

Celebrating 40 years of the ICO

Table of Contents

Title: How can Privacy Power the AI Revolution?
All-Party Parliamentary Group on Artificial Intelligence (APPG AI)
Date of Publication: June 2025
Publication Type: Parliamentary Brief | Policy Brief
Publisher: Big Innovation Centre

INTRODUCTION

This document is a transcript and summary of an APPG AI evidence meeting that took place on 12 May 2025 in the House of Lords Committee Room 1, UK Parliament. It exclusively contains crucial discussion elements; not all points are addressed.

DETAILS

Parliamentary Celebration Breakfast with the ICO

- **Date**: Thursday, 5 June 2025
- **Venue**: The Terrace Pavilion, House of Commons, Palace of Westminster
- **Time**: 8.45am to 10.45am

CONTACT THE SECRETARIAT

appg@biginnovationcentre.com
APPG AI Secretariat
Big Innovation Centre

HOSTS AND ORGANISERS

Hosts: **Dawn Butler MP** (APPG AI Vice Chair) with **The Lord Clement-Jones CBE** (APPG AI Co-Chair), in the company of The Information Commissioner of the ICO **John Edwards.**

Organisers: **Professor Birgitte Andersen**, CEO Big Innovation Centre, APPG AI Secretariat, and **John Owen**, Group Policy Director at ICO.

EVIDENCE GIVERS

- Lewis Keating, Trustworthy AI Lead UK, Director, Deloitte LLP
- Tamara Quinn, Knowledge Lawyer Director UK, Osborne Clarke
- Jonny Hoyle, Development Lead, North Yorkshire Council
- Amit Kumar, Head of Data, Privacy, and AI Risk, Santander

How can Privacy Power the AI Revolution?

Parliamentarians, industry leaders, and key figures from the public and private sectors and civil society came together for a breakfast reception on the House of Commons Terrace Pavilion, where a series of provocative short talks and discussions were hosted, alongside questions from the audience on privacy and its role in AI innovation.

Marking 40 years of data protection law, the ICO reflected on what the past four decades have shown about how privacy and building public trust have been central to the success of technological change. Attendees also heard about the ICO's ongoing work and how it is helping organisations to innovate and responsibly unlock the full potential of AI.

The event also showcased the ICO's launch of its new "AI and Biometrics Strategy".

Key Question: How can privacy power the AI revolution?

Sub Questions:

- Learning from the Past: What do the last 40 years of tech and data use teach us about innovating responsibly with AI?
- Trust in Technology: How can we build and keep public trust in AI across public services and business?
- The Future of Innovation & Privacy: What are the key opportunities and risks for AI and privacy in the years ahead?
- Collaborative Governance: How can industry, regulators, civil society, and Parliament work together to guide AI responsibly?

From left to right:

Yogesh Joshee, CEO GenAirate Technologies Ltd
Lord Ranger, APPG AI Vice Chair
Lord Clement Jones CBE, APPG AI Co-Chair
Jonny Hoyle, Development Lead, North Yorkshire Council
Amit Kumar, Head of Data, Privacy, and AI Risk, Santander
Tamara Quinn, Knowledge Lawyer Director UK, Osborne Clarke
Lewis Keating, Trustworthy AI Lead UK, Director, Deloitte LLP
John Edwards, The Information Commissioner of the ICO
John Owen, Group Policy Director at the ICO
Dawn Butler MP, APPG AI Vice Chair
Prof Birgitte Andersen, APPG AI Secretariat, Big Innovation Centre
Esra Kasapoglu, Director AI & Data Economy, Innovate UK
David Elcombe, CEO WindWorkX
Yauheniya Tyler, Founder & CEO, Uptitude
Dr Mona Ashok, Ass Prof of Digital Transformation, Uni. of Reading

Images from APPG AI events are available on the APPG AI Pavilion - please refer to page 38.

The Information Commissioner:
John Edwards

Host Of Event
APPG AI Vice Chair:
Dawn Butler MP

APPG AI Chair:
Lord Clement-Jones
CBE

APPG AI Secretariat:
Prof. Birgitte
Andersen

Group Policy
Director at ICO:
John Owen

How can Privacy Power the AI Revolution?

PANEL

Evidence Giver:
Lewis Keating
Deloitte

Evidence Giver:
Tamara Quinn
Osborne Clarke

Evidence Giver:
Jonny Hoyle
North Yorkshire Council

Evidence Giver:
Amit Kumar
Santander

FINDINGS
AND
DISCUSSION

Dawn Butler MP

APPG AI Vice Chair
Event Host

Our host, Dawn Butler MP, opened the event by welcoming the ICO's "AI and Biometrics Strategy", highlighting its importance in building public trust while enabling the safe and ethical development of AI.

"In medicine, for a long time, the research and data that doctors and hospitals relied on was largely based on white men — sometimes a couple of thousand cases of white men. But that means the findings weren't directly applicable to women or to people of colour. Now, if you build AI systems on that same biased data, those biases get baked into the technology automatically. That's why we need a very deliberate, intentional agenda to make sure AI works fairly for everyone."

Dawn Butler is particularly highlighting the danger of biased training data in AI — especially when it affects health outcomes — and calling for a proactive approach to make AI systems more inclusive and equitable.

- **Medical data bias:** Historically, much medical research and clinical trials were conducted primarily on white men. That means the data used to determine treatments, diagnoses, or drug safety often didn't fully represent women or people of colour.
- **AI inherits this bias:** If AI systems are trained on that kind of biased data, they risk reproducing or amplifying inequalities. For example, an AI diagnostic tool might perform well on white men but poorly on women or ethnic minorities because the system hasn't "seen" enough representative data.
- **Need for inclusivity:** Butler is stressing that AI in healthcare (and beyond) must be developed with a "hacked" or very deliberate agenda to counteract these biases, so the technology works fairly for everyone.

Dawn Butler showed strong support for the ICO's strategy on data privacy and responsible innovation, praising its role in strengthening public trust and creating the conditions for AI to flourish responsibly.

She also reminded us that AI trained mainly on data dominated by white men risks embedding inequality, making it all the more essential to design systems that are fair, inclusive, and truly representative of everyone.

John Edwards

The Information Commissioner

40 Years Celebration & Launching the “AI and Biometrics Strategy” of the ICO.

Privacy is the foundation of public trust, and trust is the enabler of AI innovation and adoption.

The ICO’s new “AI and Biometrics Strategy” seeks to provide guardrails, guidance, and statutory frameworks so organisations can innovate responsibly while protecting people’s rights

We are celebrating 40 years of the ICO. There’s a wonderful energy in this room, and I hope to capture and ride that energy rather than drain it as I introduce this session and our new AI and biometrics strategy.

Thanks and Welcome

Thanks to our hosts, the APPG AI. It is wonderful to have such a diversity of representation here today – from industry, civil society, lawmakers and parliamentarians, and many centres of interest. If you are here today, one thing is clear: you are invested in, and likely excited by, the transformative opportunities that AI presents.

AI as a Transformative Force

AI is no longer the prerogative of Silicon Valley giants or multinational corporations with vast budgets. The whole economy has woken up to the power of AI to drive responsible innovation. This is why it is so promising to see engagement today on the role that privacy plays in supporting these opportunities.

Building on Public Trust

Opportunities must be built on a foundation of public trust. People need to trust that organisations are using their personal information responsibly so that they feel empowered to engage with AI-driven products and services, fuelling further growth and investment.

Forty Years of the ICO

Since the ICO's inception in 1984, new technologies have continually transformed our ideas of privacy. From mobile phones and smart devices to AI chatbots and social media, we are sharing more personal information than ever before, in ways unimaginable 40 years ago. Yet the same data protection principles apply today as they always have: people must use personal information responsibly.

Guardrails, Not Roadblocks

Public trust is not threatened by new technologies themselves, but by technologies deployed without the necessary guardrails. As the ICO has done for 40 years, we are here to make compliance easier and ensure guardrails are in place so organisations can innovate and invest in AI while keeping people safe and respecting their rights.

Our Track Record on AI and Biometrics

Our focus on AI and biometrics is not new. From intervening in facial recognition in schools, to investigating police gang matrices that jeopardised trust, our history has prepared us to take emerging technologies in stride. We have acted swiftly to provide clarity in new areas, for example, intervening with Snap AI, Checkpoint, and Circle Leisure, and stopping the misuse of biometric technologies to monitor employees.

Launching the New Strategy

Today we are launching our "AI and Biometrics Strategy", setting our direction of travel for the next year. We will ramp up our scrutiny across the AI ecosystem, particularly where there is both potential for public benefit and real risk of harm.

People's Expectations

People expect to understand when and how AI affects them, and they are concerned about the consequences when things go wrong – whether being misidentified by facial recognition or unfairly losing out on a job.

Key Elements of the Strategy

Our new strategy includes:

- Developing a statutory code of practice for organisations deploying AI.
- Setting expectations for automated decision-making in recruitment and public services.
- Ensuring AI foundation models are developed lawfully.
- Overseeing the use of facial recognition by police, ensuring it is fair and proportionate.

Responsible Deployment

AI tools are still in early maturity. While they may seem simple, they can introduce serious risks when used in complex social contexts. We urge organisations to use our guardrails – guidance, innovation services, and data protection impact assessments – to deploy responsibly, on a foundation of trust.

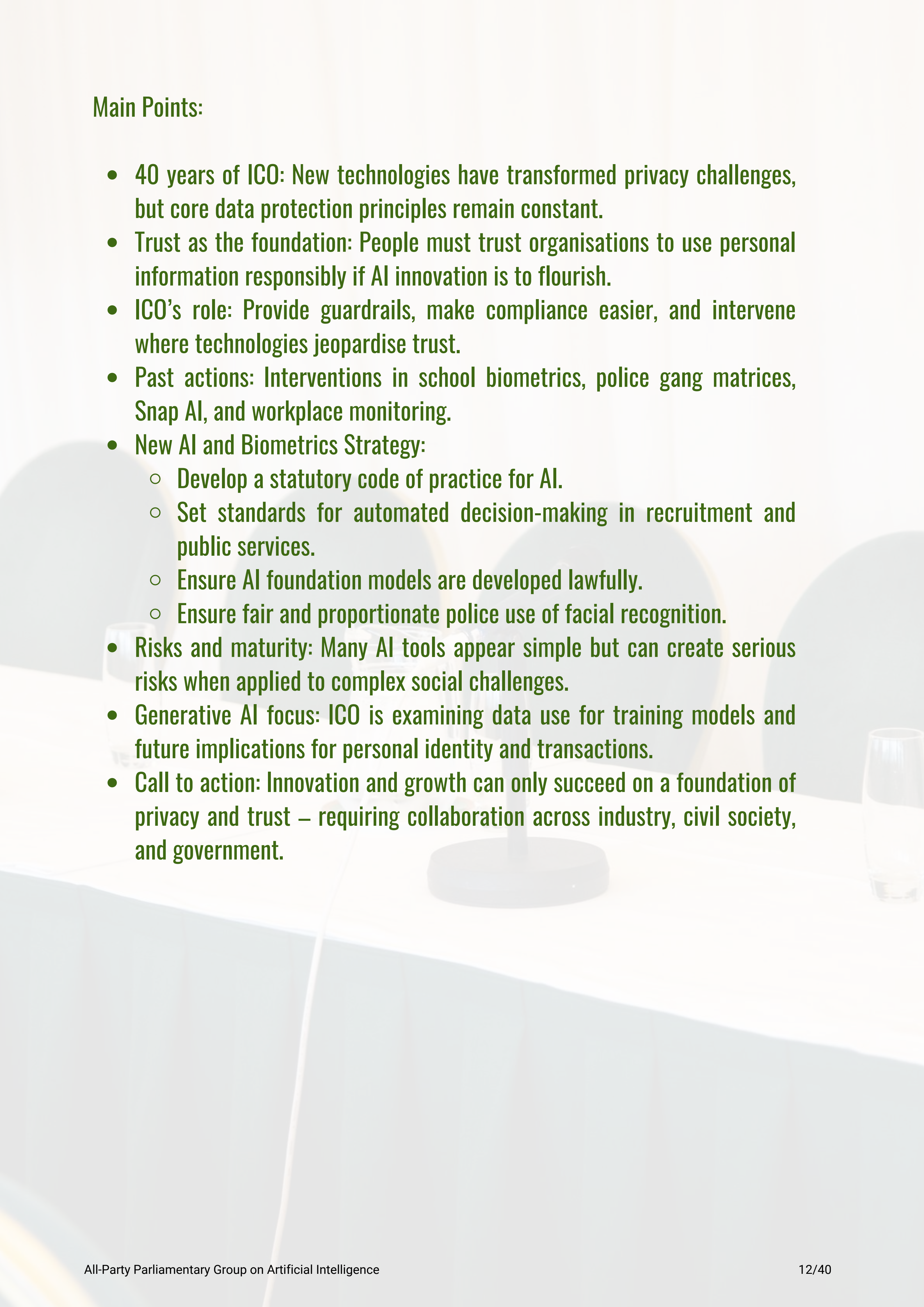
Generative AI – The Next Chapter

Generative AI is the next chapter. We are already scrutinising how firms plan to use public data to train models, and we are exploring the profound implications of systems capable not just of writing your shopping list, but of accessing your ID and payment details to place an order.

A Call for Collective Effort

Innovation and growth can go hand in hand with keeping people's data safe. But this requires collective effort. With the support of everyone in this room, the UK can position itself as a privacy-respectful place to develop and use AI.

Thank you.



Main Points:

- 40 years of ICO: New technologies have transformed privacy challenges, but core data protection principles remain constant.
- Trust as the foundation: People must trust organisations to use personal information responsibly if AI innovation is to flourish.
- ICO’s role: Provide guardrails, make compliance easier, and intervene where technologies jeopardise trust.
- Past actions: Interventions in school biometrics, police gang matrices, Snap AI, and workplace monitoring.
- New AI and Biometrics Strategy:
  - Develop a statutory code of practice for AI.
  - Set standards for automated decision-making in recruitment and public services.
  - Ensure AI foundation models are developed lawfully.
  - Ensure fair and proportionate police use of facial recognition.
- Risks and maturity: Many AI tools appear simple but can create serious risks when applied to complex social challenges.
- Generative AI focus: ICO is examining data use for training models and future implications for personal identity and transactions.
- Call to action: Innovation and growth can only succeed on a foundation of privacy and trust – requiring collaboration across industry, civil society, and government.

The Lord Clement-Jones CBE

APPG AI Co-Chair
Life Peer, House of Lords

Privacy is not a barrier but a precondition for sustainable AI. Only by embedding privacy into governance can we preserve public trust, protect rights, and enable legitimate, long-term innovation.

AI, Privacy and Urgency

Thank you very much indeed, Dawn Butler MP, and thank you, John Edwards (The Information Commissioner), and thank you to the Big Innovation Centre for organising the launch of the "AI and Biometrics Strategy". *The box office was clearly busy this morning, even at breakfast time!*

Trust-Building Moment

Welcome to everyone here today. I am the Co-Chair of the All-Party Parliamentary Group on AI. I want to say how much I appreciate the remarks John Edwards has made today – remarks that I would describe as trust-building. His introduction marks an important moment: the launch of the AI and Biometrics Strategy.

Speed and Risk

This launch is not just an opportunity to look back, but also, as John Edwards has done, to look forward at what lies ahead. We face unprecedented challenges and opportunities, with AI evolving at an extraordinary speed – from generative models to autonomous systems. But with speed comes complexity, and with complexity comes risk.

Innovation Needs Trust

We must ensure that innovation is not pursued at the expense of public trust, individual rights, or democratic values.

Biometrics on the Rise

We are seeing the rapid growth of AI-enabled biometrics – from identity verification, border management, and law enforcement, to recruitment and private sector applications such as age assurance and cashless payments. We are moving towards a biometrically enabled migration and border system. Police and private entities are already deploying facial recognition technologies, both live and retrospective. These developments raise serious concerns about proportionality, accuracy, and public acceptance.

Welcoming ICO Action

That is why I very much welcome the ICO's initiative. The strategy carries strong messages not only about public trust but also about business certainty. Businesses need clarity and predictability when interpreting our data protection laws.

Privacy Powers Progress

Let me emphasise this point: privacy is not a barrier, it is an enabler. It is tempting to see privacy merely as a compliance issue, something to be managed or mitigated. But privacy is in fact a precondition for sustainable AI adoption. Without it, we will lose public trust and confidence. While AI can unlock extraordinary innovation, it must do so with legitimacy – and that legitimacy depends on privacy and trust.

Collaboration is Key

I have long argued, both in the House of Lords and through successive data protection bills, as well as through the APPG on AI, that preserving public trust is absolutely crucial. We achieve this by working together: regulators, industry, Parliament, and civil society. Increasingly, parliamentarians are concerned about the downstream impact of legislation, and we need adaptive frameworks to respond effectively.

Governance That Works

Adaptability, ethical principles, and joined-up thinking must be the hallmarks of governance in the digital age. That is why today's strategy is so significant.

The Questions Ahead

I look forward to seeing the actions that John Edwards and the ICO will now take forward. And I am equally looking forward to today's panel, where we will ask:

- How can privacy power the AI revolution?
- What do the last 40 years tell us about responsible innovation?
- How do we build trusted AI across sectors?
- And how do we get governance right before it's too late?

Main Points:

- The launch of the ICO's "AI and Biometrics Strategy" is at a critical moment, with foresight into significant challenges ahead, as well as opportunities.
- AI's speed and risks: With rapid advances (from generative AI to biometrics), complexity and risk grow alongside opportunity.
- Biometric applications:
    - Expanding use in identity verification, border management, law enforcement, recruitment, and private commerce.
    - Raises concerns about proportionality, accuracy, and public acceptance.
- Privacy as enabler:
    - Not just about legal compliance or a business burden.
    - A precondition for trust, legitimacy, and adoption.
    - Without it, innovation will fail to gain societal acceptance.
- Need for adaptive governance:
    - Frameworks must be flexible, ethical, and joined-up across regulators, industry, Parliament, and civil society.
    - Legislation should consider downstream impacts.
- Call to action: To build trusted AI across sectors, we must put governance in place urgently, before it is too late.

Lewis Keating

Trustworthy AI Lead UK, Director, Deloitte LLP

Lewis Keating argues that trust is the key enabler of AI adoption. Without public confidence that AI is being used responsibly, people will not engage with it, and society will miss out on its economic and social benefits. Transparency and privacy are essential to building this trust. Far from being barriers, responsible AI governance and practices can accelerate innovation and adoption by creating confidence in AI systems.

Opening Remarks

Thank you, Dawn Butler MP, thank you, APPG AI Co-Chairs, and thanks to the ICO - and to all who are here today. I am already looking forward to reading the ICO’s “AI and Biometrics Strategy” information. These are really interesting and exciting areas, and I am delighted to be here to share my personal perspective on this important future and to hear from others as well.

The Trust Challenge

My organisation recently published its “Trust in the era of Generative AI” research. It found that only 50% of citizens trust businesses and organisations to use AI responsibly. This means, of course, that 50% do not.

If we are to realise the benefits that generative AI can bring – both economic and social – then this figure quite simply needs to increase. If people do not trust AI, they will not use it. And if people do not use it, we will collectively miss out on the opportunities.

Real-World Consequences of Poor AI Deployment

I have seen multiple examples where companies have deployed AI that has not had the desired impact:

- Chatbots are causing customer frustration.
- Recruitment tools which people believe are biased.
- Simple prediction models which employees are not trained effectively to use.

All of these examples risk decreasing adoption.

Data Privacy and Transparency

Data privacy is now so deeply ingrained in the public consciousness that there is an expectation people should know how their data is being used. There is an expectation that organisations will provide a higher level of transparency.

If they do not, it risks harming citizens’ trust in AI. Fundamentally, this will be a barrier to adoption, which no organisation wants.

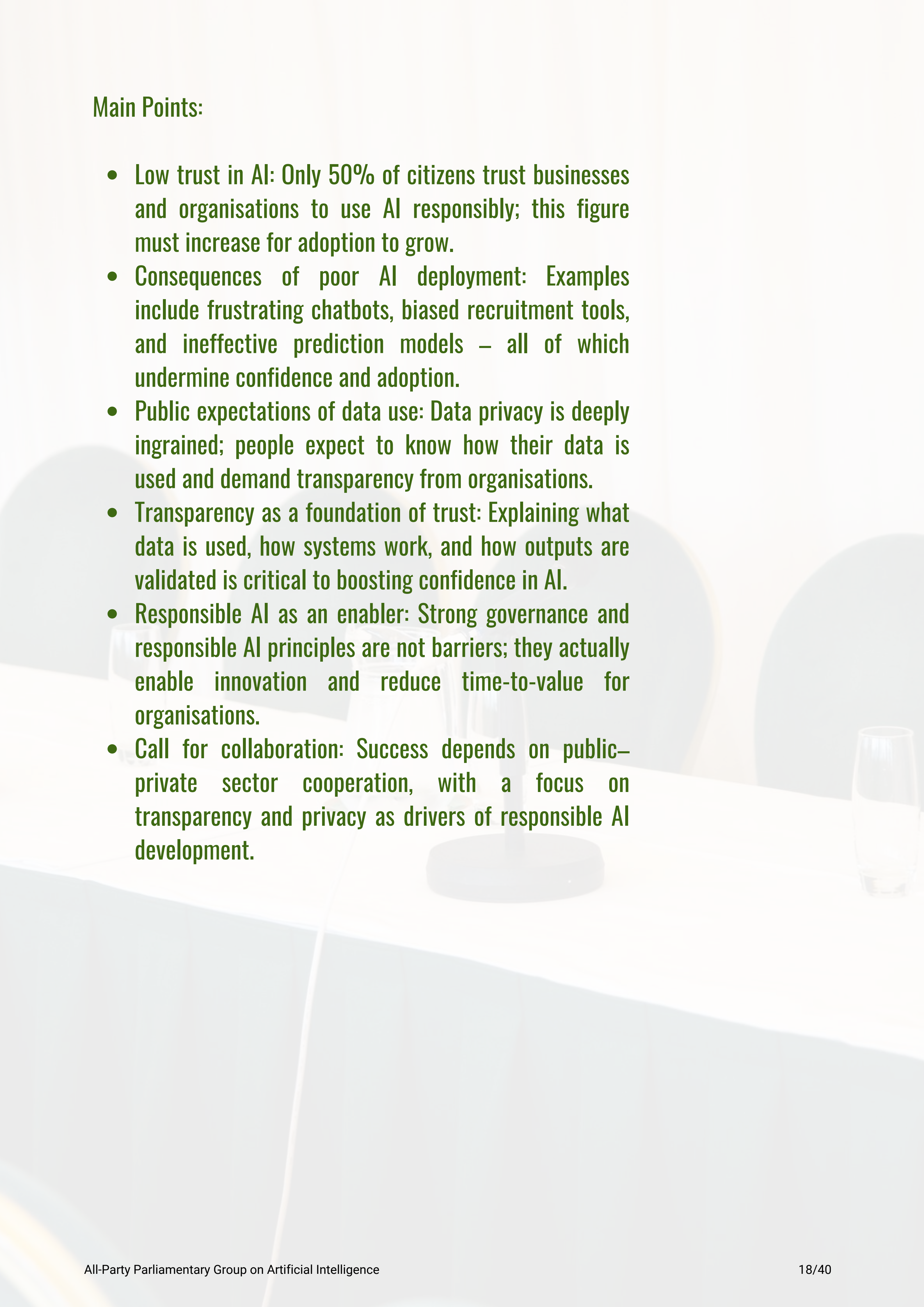
In my view, increasing transparency about an AI system – the data it uses, how it works, and how there can be adequate confidence in its outputs – is critical to increasing trust in AI.

Responsible AI as an Enabler

In turn, this sets the platform for enabling responsible AI adoption. I do not believe that AI governance and responsible practices are a barrier to adoption. On the contrary, good AI governance and truly responsible AI principles enable, rather than stifle, innovation. They can reduce the time it takes for organisations to see value.

Conclusion

To conclude, with the right focus, collaboration between the public and private sectors, and with dual responsibility, we can ensure that, through transparency, privacy really can power responsible AI development for years to come.



Main Points:

- Low trust in AI: Only 50% of citizens trust businesses and organisations to use AI responsibly; this figure must increase for adoption to grow.
- Consequences of poor AI deployment: Examples include frustrating chatbots, biased recruitment tools, and ineffective prediction models – all of which undermine confidence and adoption.
- Public expectations of data use: Data privacy is deeply ingrained; people expect to know how their data is used and demand transparency from organisations.
- Transparency as a foundation of trust: Explaining what data is used, how systems work, and how outputs are validated is critical to boosting confidence in AI.
- Responsible AI as an enabler: Strong governance and responsible AI principles are not barriers; they actually enable innovation and reduce time-to-value for organisations.
- Call for collaboration: Success depends on public–private sector cooperation, with a focus on transparency and privacy as drivers of responsible AI development.

Tamara Quinn

Knowledge Lawyer Director UK, Osborne Clarke

On AI and data knowledge – we strongly welcome the "AI and Biometrics Strategy" of the ICO. I want to highlight one particular area of AI that I believe requires very careful calibration of data protection regulation – hyper-personalisation.

The Promise of Hyper-Personalisation

We are all familiar with personalisation – for example, being targeted with product recommendations. But developments in AI are taking this to an entirely new level:

- Use of vast real-time data.
- Predictive analytics systems.
- Building profiles from ever-increasing amounts of personal data.

Tamara Quinn argues that hyper-personalisation is one of the most powerful yet risky developments in AI. It holds enormous promise in fields like healthcare and education, but also carries significant dangers if used manipulatively.

The central challenge is regulatory: finding the right balance between protecting individuals and society while not stifling innovation or overburdening businesses.

This presents a huge opportunity for organisations. There are many positive use cases:

- **Healthcare:** Personalised treatments tailored to the specific disease-causing agent, with drug delivery customised to the individual.
- **Education:** Personalised tutoring that analyses not only a student's answers, but how those answers are given – their speed, hesitation, and approach – enabling timely and tailored interventions.
- **Everyday applications:** AI could potentially pick up cues from voices, faces, or physical expressions to recommend supportive interventions.

The Risks of Hyper-Personalisation

However, hyper-personalisation could also be used for much less desirable purposes:

- Exploiting vulnerabilities.
- Using manipulative techniques.
- Amplifying misinformation or false content, targeted at individuals whose profiles suggest they may be susceptible.

This, in turn, risks deepening societal divisions and mistrust.

The Regulatory Challenge

Given the speed and breadth of AI developments, regulators face an enormous challenge. The key is to create regulation that is:

- **Well-balanced:** reducing harmful or undesirable practices.
- **Supportive of innovation:** avoiding stifling creativity and progress.
- **Business-friendly:** avoiding excessive compliance burdens.

It is not easy, but this is where a strong strategy can really help.

Main Points:

- Hyper-personalisation as the next frontier: Moving beyond simple recommendations to real-time, highly tailored interventions using vast amounts of personal data.
- Positive applications:
  - Healthcare – personalised treatments and drug delivery.
  - Education – personalised tutoring based on detailed learning behaviours.
  - Everyday interventions – detecting cues from voice and facial expressions.
- Negative risks:
  - Exploiting user vulnerabilities.
  - Manipulative techniques targeting individuals.
  - Amplification of misinformation, fuelling division and mistrust.
- Regulatory challenge:
  - Keep pace with rapid AI development.
  - Strike the right balance – reduce harms without stifling innovation.
  - Avoid excessive compliance burdens on businesses.
- Conclusion: Effective strategy and well-calibrated data protection regulation are essential to maximise the benefits of hyper-personalisation while minimising the risks.

Amit Kumar

Head of Data, Privacy, and AI Risk, Santander

Amit Kumar argues that AI risk management must move beyond theory to practical, use-case-driven governance. While regulation and privacy frameworks already exist, the real challenge is applying them effectively as technology evolves rapidly. The key is defining risk appetites, ensuring controls keep pace, and focusing on real customer outcomes rather than abstract models.

Introduction

I first trained as a mathematician, working on building models and neural networks. Now, at Santander, I look at data, privacy, and AI risk. My work focuses on developing a governance framework for the bank, bringing to light the real risks we face as AI is generated and deployed.

Navigating the Hype Cycle

When working with Generative AI models, the underlying approach is not entirely new. We have long used parameter-based models to predict what will happen next. But, as with many technologies, the adoption follows a pattern:

- First: People overestimate the hype.
- Then: There is a reality check.
- Now: We are at the “slope of enlightenment” – navigating what the real risks are and what is relevant for customers and users.

Use Cases and Practical Risks

What matters is not theory, but practical, real-world use cases. For example, when creating a customer service agent powered by AI:

- Is it simply drawing from a preloaded script and summarising?
- Or is it generating data in real time?
- What outcome do we want, and what risks come with it?

Everyone relates to risks around personal data, cyber security, and prompt injections. But the important question is: what controls do we have in place, and how do they work in practice? This is what gets us over the line – ensuring residual risk is managed through a clear set of controls.

The Challenge of Fast-Moving Technology

The most difficult aspect of generative AI is the pace of technological change. We are moving rapidly from retrieval-augmented generation to advanced neural networks, and the control mechanisms must evolve at the same speed. This is rarely the case in technology.

We've seen it before: with the emergence of cloud computing, adoption and regulation took decades to settle. For AI, the scale, deployment, and risks look very different – and the adaptation must be faster.

Regulation and Practicality

I believe regulation is good – we already have strong frameworks in privacy and risk (for example, SS1/23 in financial services). The challenge is how to apply regulation to real-world use cases.

- If regulation remains theoretical, buried in papers and documentation, it won't be effective.
- We need use case–based regulation, tailored to applications.
- Banks, for example, must define their own risk appetite for accuracy thresholds and model reliability, and move forward from there.

Conclusion

AI raises difficult questions, but privacy and responsible governance can provide the answers. By focusing on practical use cases, applying regulation realistically, and keeping pace with technological change, we can manage risk and still harness the value of AI.

Main Points:

- Technology hype vs. reality: We are moving past inflated expectations into a phase of identifying real risks.
- Focus on use cases:
    - Example: customer service chatbots – are they summarising scripts or generating new responses?
    - Outcomes must be clear, and risks assessed accordingly.
- Personal data and security:
    - People relate to risks around personal data misuse, cyber threats, and prompt injections.
    - Privacy controls are the key enablers of safe AI.
- Pace of change:
    - Technology is evolving too quickly for traditional controls.
    - Regulators and businesses must adapt faster than with past technologies (e.g., cloud).
- Regulation must be practical:
    - Frameworks exist (e.g., privacy law, SS1/23 for banks).
    - But they must be applied in a use case–specific way, not just in theory.
- Risk appetite:
    - Each bank or organisation must define acceptable thresholds for model accuracy and reliability.
- Conclusion: Managing AI risks effectively requires pragmatic, applied regulation, evolving controls, and a focus on customer outcomes.

Jonny Hoyle

Development Lead, North Yorkshire Council

Jonny Hoyle argues that AI and technology in social care must be implemented with a focus on humanity and compassion.

While regulation and high standards are essential, technology should be seen as an opportunity to make processes more humane – helping people access meaningful information, protecting children, and improving outcomes. The real challenge lies in asking the right questions, balancing risk with opportunity, and ensuring technology supports rather than harms human dignity.

As a social worker, I probably bring a rather different perspective.

Some of the most important – and traumatic – moments of my life are captured, stored, and accessible to me in my records. That carries a huge responsibility. Now, as a social work leader, I also hold that responsibility for the children we are trying to keep safe.

Regulation as Brakes on a Car

I often use an analogy you may know: good regulation and guidance are like the brakes on a Formula One car.

- One view is that brakes slow you down.
- The other view is that brakes are what enable the car to travel at 200 miles per hour safely.

This is how we should think about regulation in technology.

Accessing Records – A Human Example

When I accessed my records, there were only a couple of things I wanted to know. Yet the only way to get that information was to receive boxes of papers, poorly redacted, and difficult to make sense of.

Some may see this as a failure of the subject access request process. I prefer to see it as someone not giving me the answer in the most responsible and humane way. If I had simply been given the clarity I needed – the right information, at the right time – I would not have had to endure that experience.

Many people across the country have been traumatised by accessing their records in this way. For most people, parents do not document every single detail of their children's lives. But for children in care, that detailed record-keeping is a reality.

This also presents an opportunity for AI – to humanise the process, help people make sense of their own stories, and connect with their heritage.

Balancing Opportunity and Risk

We must strike a balance. We need to ask difficult questions, challenge one another, and ensure that we end up in the right place.

For example, we discussed whether AI could be used to generate "ego maps" of people around children:

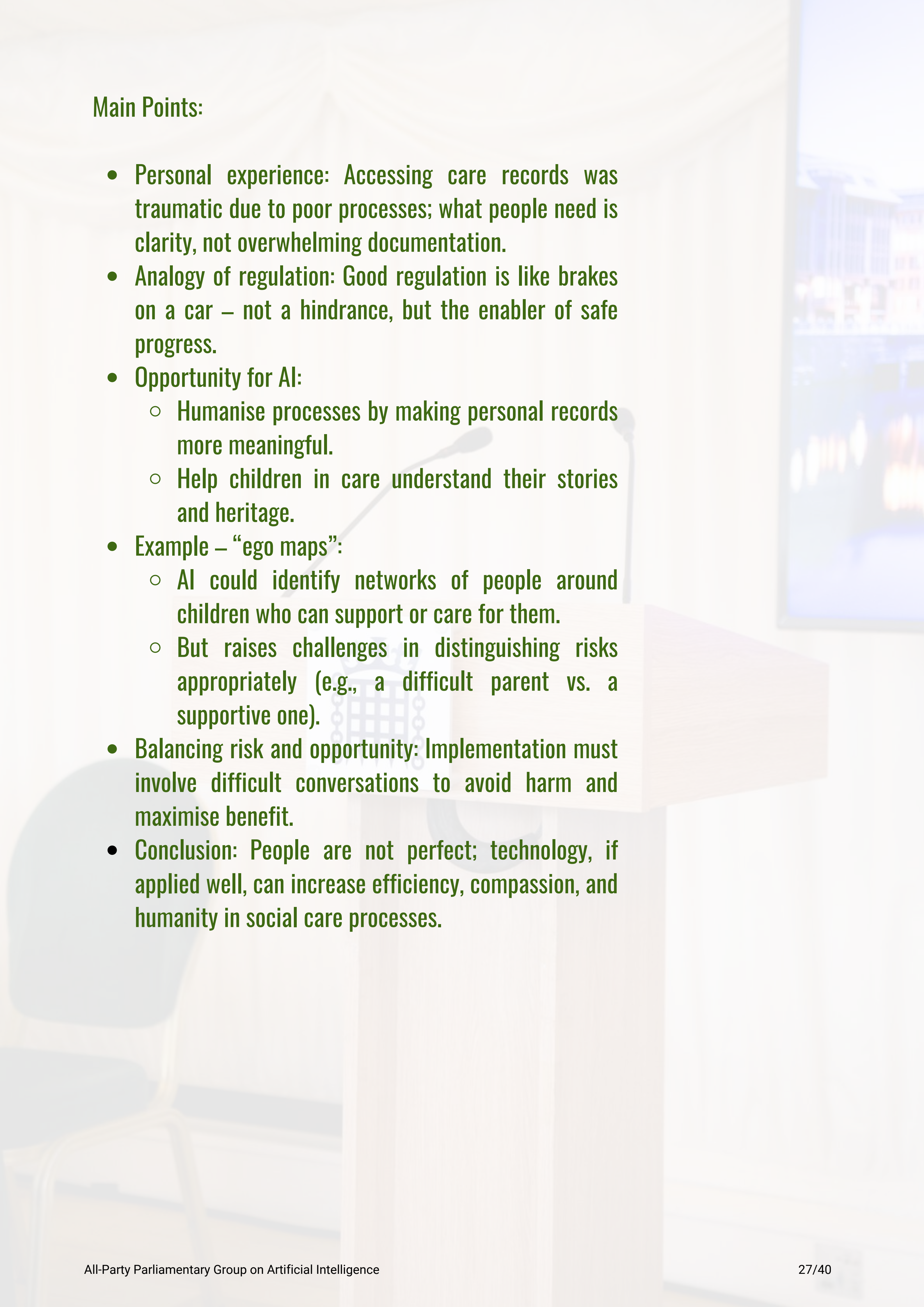
- **The opportunity:** to identify people connected to a child who could help keep them safe or even provide care if they cannot remain at home.
- **The challenge:** ensuring technology does not overstep – for instance, wrongly categorising someone as a risk, or failing to distinguish between a "difficult parent" and a parent simply paying for additional services for their child.

These are exactly the types of conversations we must have when implementing technology.

Conclusion

It is right to hold technology to very high standards – as today's discussions have shown. But it is also important to remember that people are not perfect either.

Technology, if implemented responsibly, can actually increase the humanity of our processes – doing things better, more efficiently, and ultimately with greater compassion.



Main Points:

- Personal experience: Accessing care records was traumatic due to poor processes; what people need is clarity, not overwhelming documentation.
- Analogy of regulation: Good regulation is like brakes on a car – not a hindrance, but the enabler of safe progress.
- Opportunity for AI:
  - Humanise processes by making personal records more meaningful.
  - Help children in care understand their stories and heritage.
- Example – “ego maps”:
  - AI could identify networks of people around children who can support or care for them.
  - But raises challenges in distinguishing risks appropriately (e.g., a difficult parent vs. a supportive one).
- Balancing risk and opportunity: Implementation must involve difficult conversations to avoid harm and maximise benefit.
- Conclusion: People are not perfect; technology, if applied well, can increase efficiency, compassion, and humanity in social care processes.

Professor Birgitte Andersen

CEO Big Innovation Centre
APPG AI Secretariat

Privacy is not a barrier to AI innovation: it is the foundation of trust that enables it.

By embedding privacy, organisations unlock the confidence to share data, drive responsible innovation, and ensure the AI revolution serves society and democracy.

Closing Reflections

As we close today’s discussion, the takeaways are clear. The Information Commissioner’s Office is not only an enforcer of compliance; it is also an architect of trust and a partner in enabling responsible innovation. By setting clear standards for explainability, consent, and the responsible handling of data, the ICO helps foster collaboration between developers, users, and citizens alike.

Privacy as a Foundation

What has become evident today is that privacy is not a barrier to progress—it is the very foundation of confidence. It is what allows us to build, to share, and to unlock the potential of our biometric data, which is so critical to the AI revolution.

Acknowledgements

On behalf of the APPG AI Secretariat, I would like to thank our host Dawn Butler MP, our co-chair Lord Tim Clement-Jones, our speakers, and of course The Information Commissioner John Edwards and the ICO for making this event possible. Special thanks also to John Owen, Group Policy Director at ICO, and his team for their excellent collaboration with APPG AI and Parliament in bringing this session together.

Before We Close

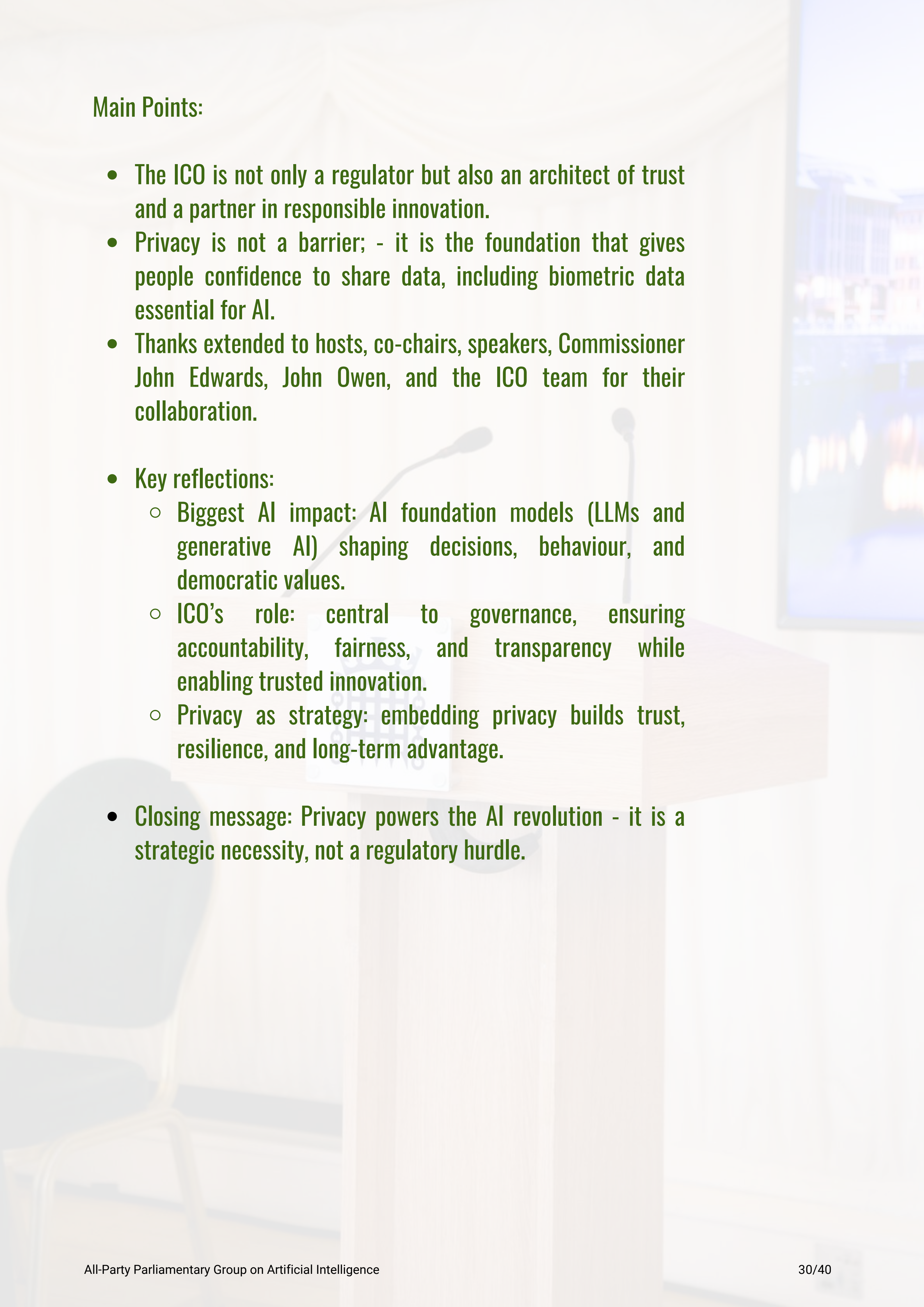
Three Reflections for the Future

First - Biggest Impact: the AI development likely to have the greatest societal impact is the integration of foundation models—large language models and generative AI—into everyday decision-making, from healthcare and education to public services. These models do not simply analyse data; they shape narratives, influence choices, and alter behaviour. The real question is not just what AI can do, but who it serves, and whether it aligns with our democratic values.

Second - An architect of trust: the role of the ICO in this landscape is fundamental. Beyond regulation, it is shaping the frameworks that guarantee accountability, fairness, and transparency. In doing so, it ensures that innovation and adoption happen faster—because they happen with trust.

Third - Privacy as a Strategic Advantage: today we have seen that privacy and innovation are not in conflict, but mutually reinforcing. Organisations that embed privacy at their core are not only more trustworthy, but more resilient and future-ready. Powering the AI revolution with privacy is not a regulatory hurdle—it is a strategic advantage.

Thank you.



Main Points:

- The ICO is not only a regulator but also an architect of trust and a partner in responsible innovation.
- Privacy is not a barrier; - it is the foundation that gives people confidence to share data, including biometric data essential for AI.
- Thanks extended to hosts, co-chairs, speakers, Commissioner John Edwards, John Owen, and the ICO team for their collaboration.

- Key reflections:
  - Biggest AI impact: AI foundation models (LLMs and generative AI) shaping decisions, behaviour, and democratic values.
  - ICO's role: central to governance, ensuring accountability, fairness, and transparency while enabling trusted innovation.
  - Privacy as strategy: embedding privacy builds trust, resilience, and long-term advantage.

- Closing message: Privacy powers the AI revolution - it is a strategic necessity, not a regulatory hurdle.

BIOs of Speakers

Dawn Butler MP
APPG AI Vice Chair

Dawn Butler MP is a British Labour Party politician and the Member of Parliament for Brent East. She previously represented Brent South (2005–2010) and Brent Central (2015–2024). Butler began her career as a trade union officer and adviser to Mayor of London Ken Livingstone. She served in Gordon Brown's government as Minister for Young Citizens and Youth Engagement, becoming the first elected African-Caribbean woman to serve as a UK government minister. A strong advocate for equality and social justice, she held several senior roles in the Labour Party, including Shadow Minister for Black and Minority Ethnic Communities and Shadow Secretary of State for Women and Equalities. Butler has been a prominent voice on diversity and inclusion in British politics.

John Edwards
The Information Commissioner of the ICO (Information Commissioner's Office)

Mr John Edwards is The Information Commissioner of the ICO (Information Commissioner's Office). He worked as a solicitor and barrister for more than 14 years, including time as a policy adviser to the New Zealand Prime Minister and Cabinet around Freedom of Information.
From February 2014 to December 2021 he was New Zealand Privacy Commissioner. During that time he chaired the International Conference of Data Protection and Privacy Commissioners (now known as the Global Privacy Assembly), and was a member of the OECD's Informal Group of Experts on Children in the Digital Environment.

The Lord Clement-Jones CBE
APPG AI Co-Chair

The Lord Clement-Jones CBE is a Liberal Democrat life peer in the UK House of Lords, a solicitor, and a leading voice on digital policy and artificial intelligence. He chaired the House of Lords Select Committee on AI and Co-Chairs the All-Party Parliamentary Group on AI. A former London Managing Partner at global law firm DLA Piper, he has also held leadership roles in health, media, and the digital economy. He is Chair of the Council at Queen Mary University of London and President of Ambitious about Autism. He was awarded a CBE for political services in 1988.

Professor Birgitte Andersen
CEO Big Innovation Centre, APPG AI Secretariat

Professor Birgitte Andersen is CEO and Founder of the Big Innovation Centre. She leads the Secretariat of the UK Parliament's All-Party Parliamentary Group on Artificial Intelligence (APPG AI). She is Professor of the Economics and Management of Innovation at Birkbeck College, University of London, and an elected Fellow of the Academy of Social Sciences. She has served as an expert defence witness in the UK Crown Court, advised international organisations and several national governments, and acted as rapporteur for the European Commission. Her expertise on AI, technology policy and IP governance is sought by BBC World and cited in outlets such as Forbes and The Guardian.

Lewis Keating
Trustworthy AI Lead UK, Director, Deloitte LLP

Lewis Keating is a Director in Deloitte Risk Advisory practice with more than 10 years' experience helping organisations of all size with Technology Risks and Controls.

He has led several assurance and advisory projects on AI Risk and AI Governance and is helping organisations work through how to manage the widespread adoption of AI in a safe and controlled manner.

Lewis leads several Internal Audit reviews on the topic of AI Risk, and his areas of interest and expertise include IT Governance, AI Risk, ML Governance, IT Strategy and IT Risk Management.

Tamara Quinn
Knowledge Lawyer Director UK, Osborne Clarke

Tamara Queen is a dual-qualified solicitor and barrister who specialises in artificial intelligence, data, emerging technologies, and non-contentious intellectual property. She leads Osborne Clarke's Knowledge team in these areas and is a key member of its international AI team.

With many years' experience advising on the protection, acquisition, sale, and licensing of IP rights, she also has deep expertise in data privacy and the legal aspects of deploying both generative and traditional AI systems. Tamara is particularly focused on the intersection of data and IP law with technologies such as virtual/augmented reality, blockchain, and robotics.
She has supported clients across a wide range of sectors — from bioinformatics, medical imaging, AI chatbots, and facial recognition, to social media, electric vehicles, gaming, real estate, and film special effects.

Tamara spent over six years as a partner in Osborne Clarke's Commercial team and held senior in-house roles, including acting head of IP at a major retailer and head of legal at a publishing company. She sits on the advisory board of the APPG on AI and is a member of the Society for Computers & Law.

Amit Kumar
Head of Data, Privacy, and AI Risk, Santander

Amit Kumar is the Head of Data Management, Data Privacy & AI Governance for Santander UK. He has more than 20 years of experience working as a Data Leader shaping the overall data strategy with a focus on end-to-end control framework across the data lifecycle, embedding a strong privacy culture and deployment of AI Governance framework to leverage the scale and impact for better customer outcomes. He has led several transformation programmes and change projects to help organisations navigate their data challenges, address regulatory requirements, drive technology & business innovation, and delivering value from the data assets by working closely with customers and business areas. He has worked across industries including retail, metals and mining, hospitality and is now working as part of the financial services industry.

As part of Santander, he is a key sponsor for one of the most critical change programmes - Stronger Data Foundations which is one of the key pillars of work to enhance customer value and provide sustainable growth to the bank in terms of new initiatives and leveraging maximum benefits from AI. He has recently also completed a course from Oxford and is now leading the AI Governance framework for the bank. Amit is a mathematician and has completed is masters in strategy and finance with a specialisation in topology and constraint analysis.

Jonny Hoyle
Development Lead, North Yorkshire Council

Jonny Hoyle is Development Lead, North Yorkshire Council. He is interested in how technology can help keep children safe, improve outcomes and benefit Social Work.

With over 17 years of experience at North Yorkshire County Council, Jonny Hoyle has built extensive expertise in children's social care, family support, and permanency planning. Currently serving as the Child Permanence and Family Reunification Development Lead since April 2021, Jonny leads the development of strategies that promote long-term stability and successful reunification for children and families.

Previously, Jonny held the role of Assistant Team Manager (2017–2021), managing social work teams and contributing to the effective delivery of services across the region. Earlier roles include Social Worker (2014–2017) and Family Support Worker (2007–2014) in the Scarborough area, working directly with families to enhance child safety and wellbeing.

Throughout his career, Jonny has demonstrated a strong commitment to improving outcomes for vulnerable children and to developing innovative, evidence-informed approaches to permanency and family reunification.

ABOUT APPG AI

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
- Damian Hinds MP Conservative
- Danny Chambers MP Liberal Democrat
- Dawn Butler MP Labour (APPG AI Vice-Chair)
- David Reed MP Conservative
- Dave Robertson MP Labour
- Esther McVey MP Conservative
- Emily Darlington MP Labour
- George Freeman MP Conservative
- Gordon McKee MP Labour
- Graham Leadbitter MP SNP
- Liam Byrne MP Labour
- Marie Goldman MP Liberal Democrat
- Martin Wrigley MP Liberal Democrat
- Mike Martin MP Liberal Democrat
- Maureen Burke MP Labour
- Peter Fortune MP Conservative
- Samantha Niblett MP Labour
- Sarah Edwards MP Labour
- Tim Roca MP Labour
- Tom Collins MP Labour
- Tom Gorden MP Liberal Democrat
- Tony Vaughan MP Liberal Democrat
- 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

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
UK RI Innovate UK
Meta
onfido
Osborne Clarke
Queen Mary University of London
Santander
UPTITUDE
UNIVERSITY OF SURREY
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!

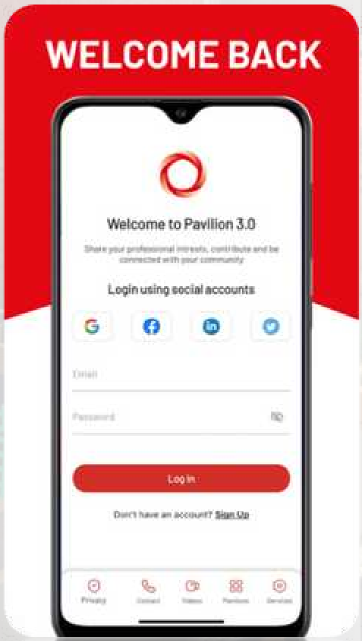
Go to APPG AI Pavilion and
click on what you are looking for.

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



WELCOME BACK

Welcome to Pavilion 3.0

Share your professional interests, contribute and be connected with your community

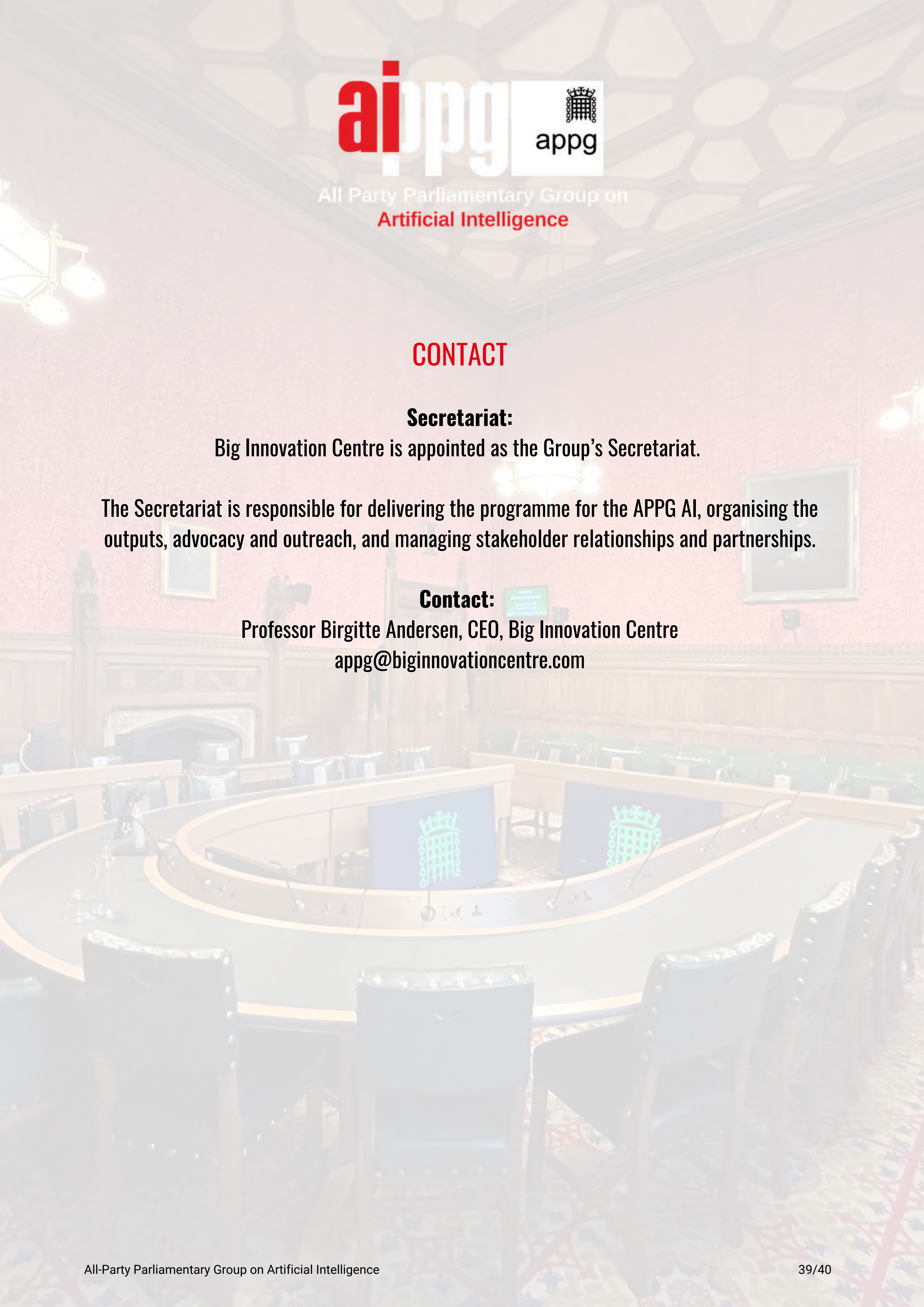
Login using social accounts

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

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.