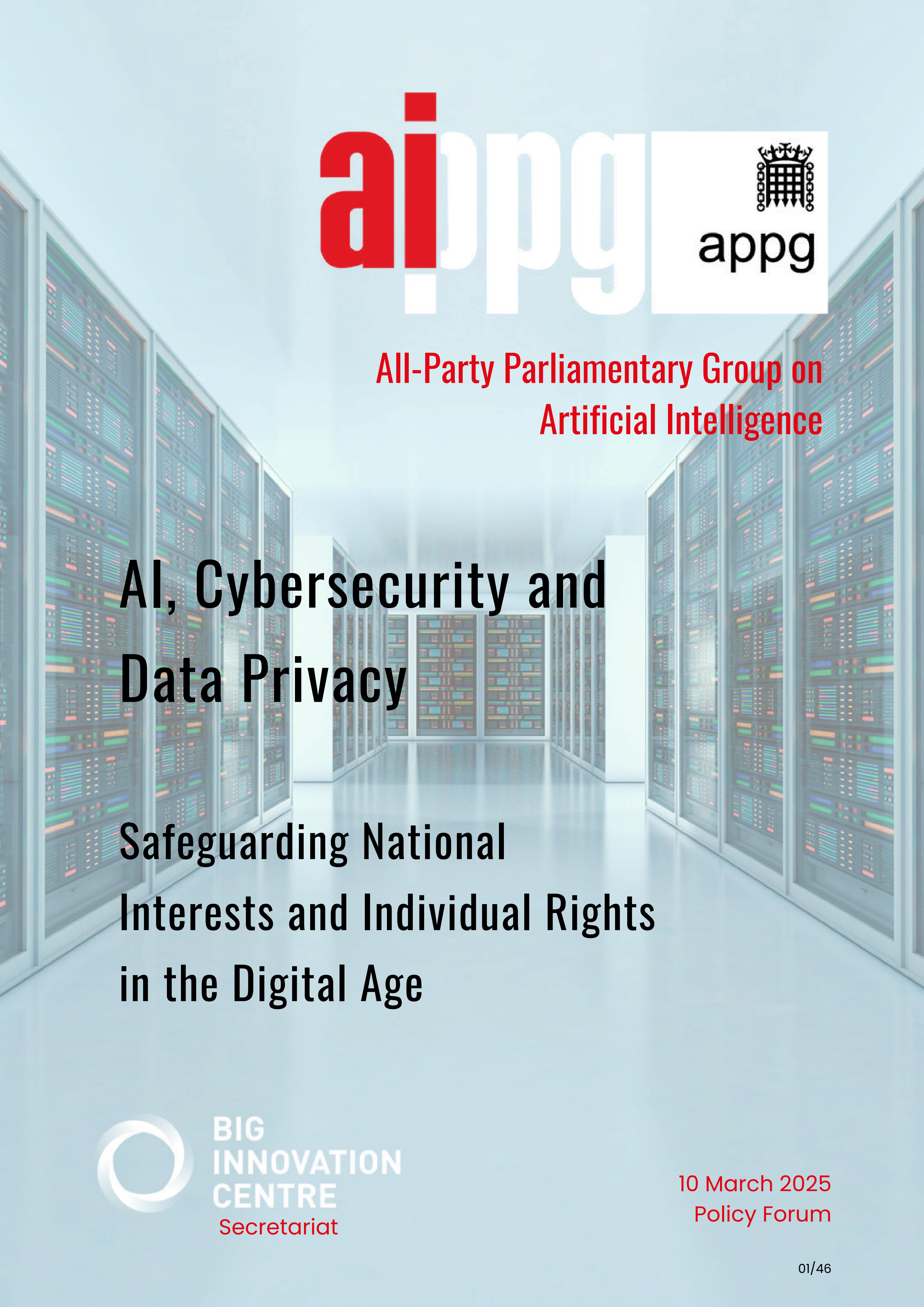


All-Party Parliamentary Group on
Artificial Intelligence

AI, Cybersecurity and Data Privacy

Safeguarding National Interests and Individual Rights in the Digital Age

BIG INNOVATION CENTRE
Secretariat

10 March 2025
Policy Forum

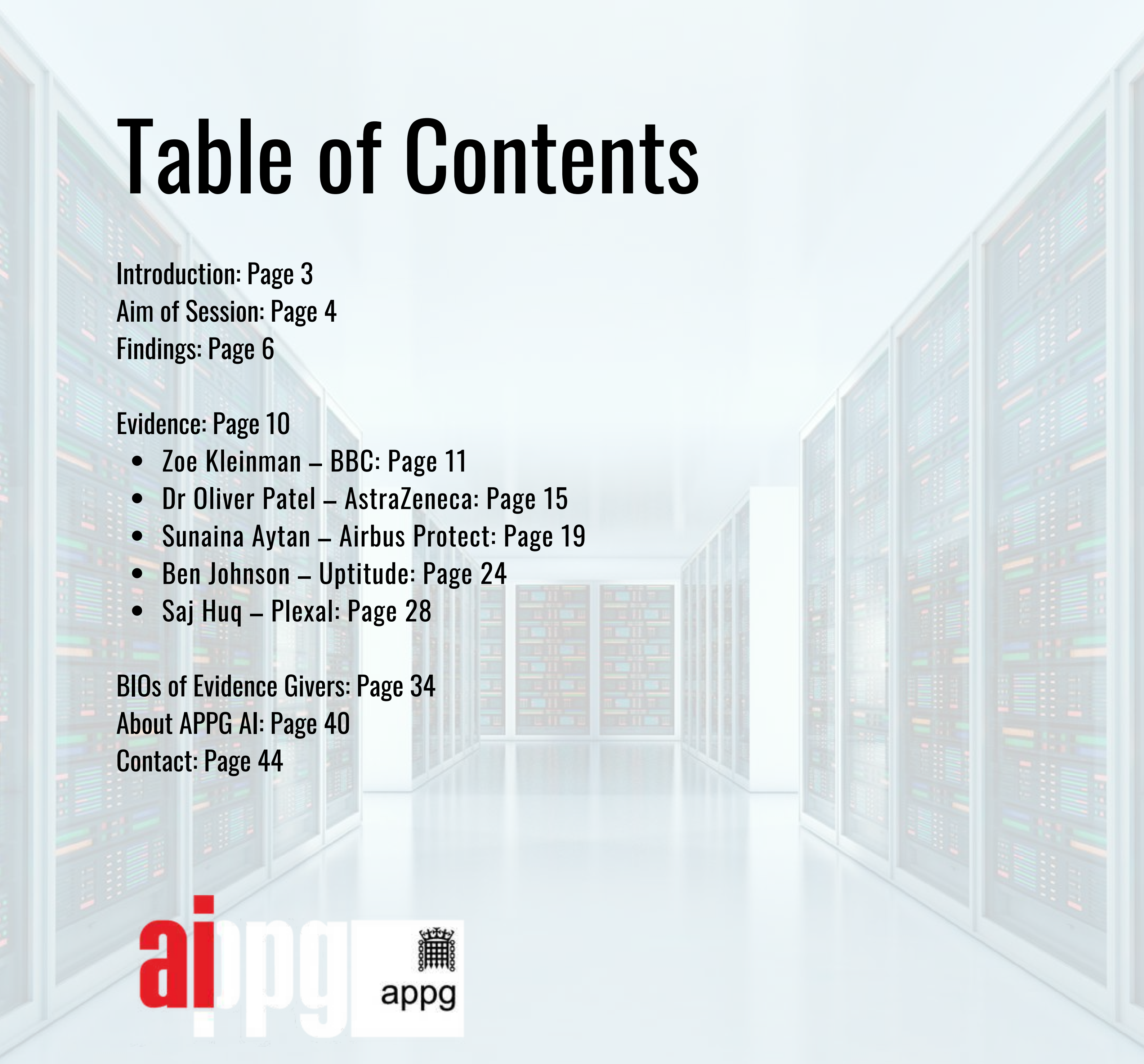


Table of Contents

Title: AI, Cybersecurity and Data Privacy: Safeguarding National Interests and Individual Rights in the Digital Age
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 transcript and summary of an APPG AI evidence meeting that took place on 10 March 2025 in the House of Lords Committee Room 2a, UK Parliament. It exclusively contains crucial discussion elements; not all points are addressed.

DETAILS

- Evidence Session: AI, Cybersecurity and Data Privacy: Safeguarding National Interests and Individual Rights in the Digital Age
- Time 5:30 pm – 7:00 pm (GMT)
- Date: Monday, 10 March 2025
- Venue: Committee Room 2a in the House of Lords.

CONTACT THE SECRETARIAT

appg@biginnovationcentre.com
APPG AI Secretariat
Big Innovation Centre

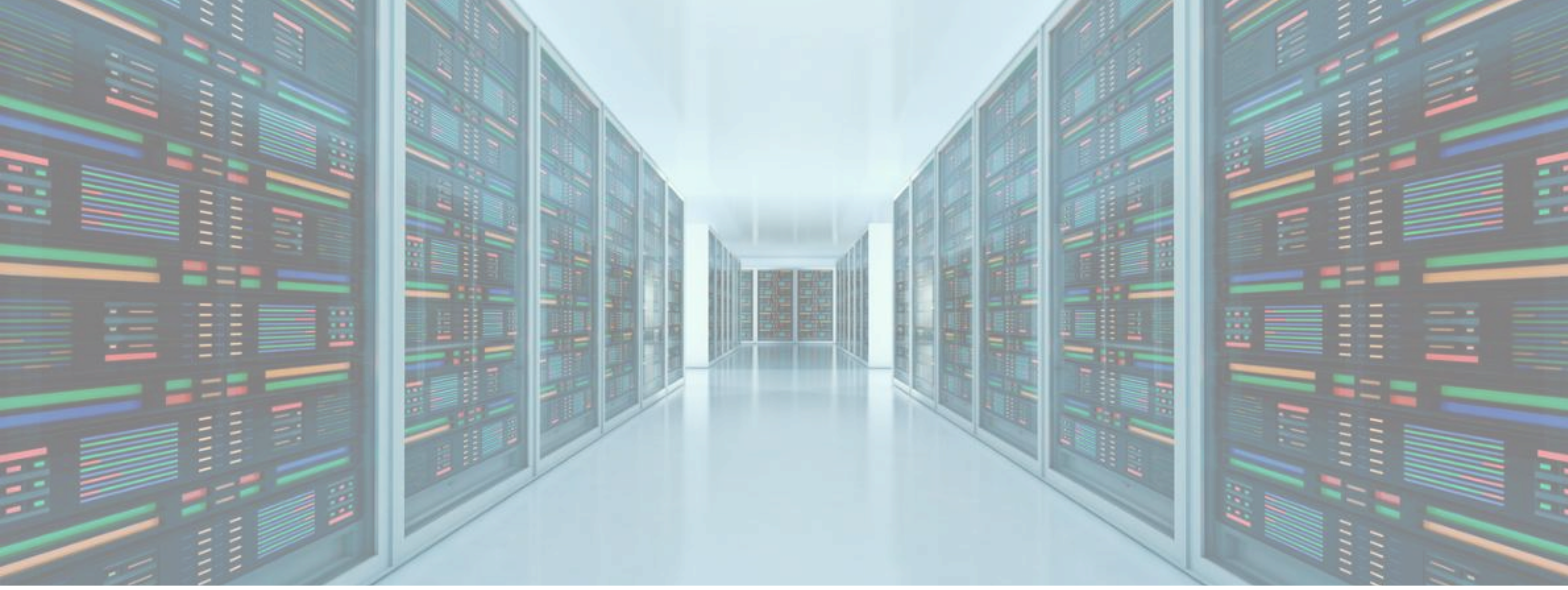
Rapporteur for this meeting: **Professor Birgitte Andersen**, CEO Big Innovation Centre

EVIDENCE GIVERS

1. **Zoe Kleinman** – Technology Editor at **BBC** News, Senior On-Air Journalist and Presenter.
2. **Dr Oliver Patel** – Enterprise AI Governance Lead, **AstraZeneca |** Member of the International Association of Privacy Professionals (IAPP) Advisory Board and the OECD Expert Group on AI Risk and Accountability.
3. **Sunaina Aytan** – Cybersecurity Consultant, **Airbus Protect |** Member of the UK Cyber Security Council and Advisory Board for Cyber London.
4. **Ben Johnson** – Co-Founder & Chief Technology Officer, **Uptitude**.
5. **Saj Huq** – Chief Commercial Officer, **Plexal** and Member, National Cyber Advisory Board.

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.



Aim of Session

AI, Cybersecurity and Data Privacy: Safeguarding National Interests and Individual Rights in the Digital Age

In this report we explore the intersection of AI, cybersecurity, and data privacy, focusing on safeguarding national interests and individual rights. Discussions cover how AI can enhance cybersecurity while mitigating associated risks, and the role of government-industry collaboration in addressing cyber threats. The session also examines regulatory frameworks needed to balance AI innovation with privacy protection, including international cooperation for a unified approach. A key focus is also synthetic data, its role in AI development, and the challenges surrounding its implementation. The meeting aims to drive policy and strategic discussions.

Questions raised to inspire the discussion:

AI in Cybersecurity and National Security

- How can AI technologies enhance cybersecurity measures and protect critical infrastructure?
- What risks arise from using AI in cybersecurity, and how can these be mitigated?
- How should governments and industries collaborate to address the evolving landscape of cyber threats?

AI and Data Privacy: Protecting Individuals' Rights and Balancing Innovation

- How can legislators balance fostering AI innovation, product development and market expansion with protecting individuals’ privacy rights?
- What regulatory frameworks are needed for the collection, use, and sharing of personal data in AI applications?
- What international collaborations and agreements are necessary to ensure a harmonised approach to AI and data privacy?

Synthetic Data

- How can synthetic data enhance the development and testing of AI models?
- What challenges do organisations face when implementing synthetic data solutions compared to using real-world data?

Above (from left to right): **Saj Huq** (Chief Commercial Officer, Plexal and Member, National Cyber Advisory Board), **Dr Oliver Patel** (Enterprise AI Governance Lead, AstraZeneca | Member of the International Association of Privacy Professionals (IAPP) Advisory Board and the OECD Expert Group on AI Risk and Accountability), **Madeline Cheah** (Associate Director and Cybersecurity Specialist, Cambridge Consultants, Capgemini), **Lord Ranger of Northwood, Lord Taylor of Warwick, Zoe Kleinman** (Technology Editor at BBC News, Senior On-Air Journalist and Presenter), **Allison Gardner MP** (APPG AI Co-Chair), **Sunaina Aytan** (Cybersecurity Consultant, Airbus Protect | Member of the UK Cyber Security Council and Advisory Board for Cyber London), **Professor Birgitte Andersen** (CEO Big Innovation Centre and APPG AI Secretariat), **Shaun O'Callaghan** (Chief Information Officer, HomesChief Information Officer, Homes, Santander UK), **Professor Ashley Braganza** (Dean, Brunel Business School), **Ben Johnson** (Co-Founder & Chief Technology Officer, Uptitude), **Markus Anderljung** (Centre for the Governance of AI), **Daniel Wilson** (Policy and Public Affairs Director, BT Group), **Laura Bishop** (AI and Cyber Sector Lead, BSI) and **Sarah Reynolds** (Partner, EY Law)

FINDINGS

ACTION FIELDS FOR POLICY AND STAKEHOLDER GROUPS

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

The Evidence Statements delved into Various Directions:

The Dynamic Convergence of AI and National Security:

- We explored how AI technologies are increasingly intertwining with national security concerns, highlighting the urgent need for stronger cybersecurity measures.

Vital Collaboration between Government and Industry:

- The emphasis was on forging powerful partnerships between the public and private sectors, showcasing how collective resources and insights can tackle cybersecurity challenges head-on.

AI's Transformative Impact on Cybersecurity:

- We examined both the risks and opportunities presented by rapid AI advancements, particularly concerning emerging cyber threats and vulnerabilities.

Strategic Investment in Cybersecurity:

- The discussion highlighted the crucial need for robust investments from both the public and private sectors to develop comprehensive cybersecurity frameworks that enhance national resilience.

Ongoing Training and Education:

- We stressed the importance of continuous training programmes that empower individuals to recognise and effectively respond to sophisticated cyber threats, including social engineering and AI-driven attacks.

Deploying Research and Development:

- The focus shifted to the UK's exceptional research ecosystem in AI and cybersecurity, discussing how integrating research findings into actionable strategies can drive impactful policies and practices.

Advocating Positive Data Usage:

- We emphasised the power of sharing personal data for the greater good, particularly in sectors like healthcare, while balancing privacy concerns with societal benefits.

Implications & Action Points for Stakeholders

Foster Collaboration:

- Stakeholders must actively foster strong partnerships between government and private sectors, pooling resources, insights, and best practices to combat cybersecurity challenges.

Champion Legislation and Strategies:

- Get on board with the UK’s cybersecurity strategy and actively advocate for supportive legislation that paves the way for innovation and collaboration in this field.

Engage with the National Cyber Security Centre (NCSC):

- Collaborate closely with the NCSC to leverage their guidance and resources, helping navigate the complexities of cybersecurity in our AI-rich era.

Invest in Empowering Workforce Training:

- Launch targeted training programmes that equip employees with the skills to recognise and confront emerging cyber threats, including those fueled by AI technology and social engineering.

Leverage Research Brilliance:

- Utilise the insights from the UK's leading research institutions to inform policies and elevate technological capabilities within the cybersecurity landscape.

Promote Positive Data Sharing Initiatives:

- Advocate passionately for the benefits of sharing individual data for public good, encouraging a balanced narrative that highlights the societal advantages alongside privacy concerns.

Drive Innovation in Cybersecurity:

- Support groundbreaking initiatives that foster innovation in cybersecurity technologies and strategies to stay ahead of the ever-evolving threats from adversaries.

By navigating these key areas and action points, stakeholders can significantly strengthen the UK’s resilience, security, and capacity to manage the complexities associated with AI and national security.

(2) The Q&A and discussion after the evidence statements raised new points and their implications:

New Points Raised from the Q&A and Discussion

Concerns About Data Handling and Privacy:

- The conversation highlighted the need for stronger collaboration and transparency regarding data handling and privacy, specifically in the context of citizen trust in organisations managing their data.

Citizen Perspective on Data Accessibility:

- Emphasising the importance of understanding how citizens perceive their data's security when interacting with services, and the necessity of building confidence amidst fears about data leakage.

Weakness in Supply Chains:

- There was an acknowledgment of the vulnerabilities within supply chains that can be exploited by attackers, emphasising that weaknesses which sub-suppliers can pose risks to larger organisations.

The Need for Education on Cybersecurity:

- A robust focus on the necessity for educational initiatives to better equip citizens to handle cybersecurity threats and to foster a culture of understanding around how data is used and shared.

Transparency in AI Models:

- The discussion raised questions on the transparency of AI systems and the responsibility of developers to provide clear information about how AI is built and operates, promoting trust in these technologies.

Interdisciplinary Collaboration:

- There was recognition of the complexity of AI systems necessitating multidisciplinary teams, and the challenges of integrating various areas of expertise (e.g., cybersecurity, biosecurity, AI) to address emerging vulnerabilities.

Focus on Agentic AI and Job Implications:

- Growing concerns were raised regarding the impact of agentic AI on entry-level positions and the future of work, highlighting the possibility of AI replacing jobs traditionally held by humans. This may influence human assessment and response to cyber threats.

Public Perception of AI’s Benefits versus Cyber Security Risks:

- The need to balance narratives around AI was discussed, ensuring that both benefits and potential threats are communicated effectively to the public.

Implications & Action Points for Stakeholders

Build Trust Through Transparency:

- Organisations must prioritise transparency about data practices to foster trust among citizens and clients.

Strengthen Supply Chain Cyber Security:

- Stakeholders should focus on securing the entire supply chain, recognising vulnerabilities in third-party partnerships.

Enhance Training and Education:

- Develop comprehensive educational programmes for employees and the public on cybersecurity and data privacy to better prepare them for potential threats.

Encourage Interdisciplinary Teams:

- Promote collaboration across different sectors and areas of expertise to effectively tackle complex challenges posed by AI and cybersecurity.

Address Future Workforce Concerns:

- Prepare for shifts in the job market due to automation and AI, concentrating on the cyber security related skills needed in the evolving landscape.

Foster a Balanced Narrative on AI:

- Create initiatives to share positive stories and clear benefits of AI technology while also addressing legitimate concerns and cybersecurity risks.

By integrating these points into their strategies, stakeholders can not only enhance their cybersecurity posture but also promote a more trustworthy and resilient AI technological environment.

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

Government Agencies:

- Departments focused on national security, cybersecurity, and technology, such as the National Cyber Security Centre (NCSC), the Government Communications Headquarters (GCHQ), the AI Security Institute (AISI), and other relevant government bodies.

Private Sector Companies:

- Businesses operating in technology, cybersecurity, AI development, and other industries that are directly impacted by and can contribute to cybersecurity efforts.

Academic and Research Institutions:

- Universities and research centres that are leading in AI and cybersecurity research, such as UK universities and the Alan Turing Institute, which can provide valuable insights and foundational knowledge.

Industry Associations and Trade Groups:

- Organisations that represent the interests of various sectors, advocating for collaborative efforts and sharing best practices regarding cybersecurity and AI adoption.

Cybersecurity Professionals:

- Individuals working within the cybersecurity domain, including IT specialists, consultants, and analysts who play a crucial role in developing and implementing security measures.

Think Tanks and Non-Governmental Organisations (NGOs):

- Groups advocating for data privacy, ethical AI usage, and cybersecurity awareness, which can help promote informed public discussions and policies.

The General Public:

- Citizens who must be educated about cybersecurity threats and the importance of data sharing for societal benefits, as well as their rights regarding personal data.

Investors and Funding Organisations:

- Entities providing financial support for innovation in cybersecurity and AI, which can influence the direction and scale of research and development initiatives.

Engaging these stakeholders collaboratively will empower them to contribute to a more resilient cybersecurity ecosystem while promoting innovation within the AI landscape.

Evidence Giver:
Saj Huq

Evidence Giver:
Sunaina Aytan

Evidence Giver:
Zoe Kleinman

Evidence Giver:
Dr Oliver Patel

Evidence Giver:
Ben Johnson

APPG AI Chair:
Allison Gardner MP

APPG AI Chair:
Lord Clement-Jones CBE

Secretariat & Rapporteur:
Professor Birgitte Andersen

EVIDENCE

Zoe Kleinman

Technology Editor at BBC News
Senior On-Air Journalist | Presenter | Thought Leader

My name is Zoe Kleinman. I'm the technology editor at BBC News, and I report on a wide range of tech-themed news stories across BBC TV, Radio, and digital platforms. I am not here to speak on behalf of the BBC today.

The AI Revolution

I've covered the beat for the last 18 years, and watching the AI revolution unfold in recent times has been an absolutely extraordinary chapter in my career. I want to talk to you about data privacy tonight because I think it's one of the biggest challenges facing the continued growth of AI, and I think it presents a considerable dilemma to both lawmakers and the industry itself.

The Importance of Data Quality

We know that an AI tool is only as good as the data on which it's trained. I'm sure you've all heard the phrase "garbage in, garbage out", and what this means is that if AI is not fed good data, it's not going to produce good output and it's not going to be as useful. Here are two examples of what I mean by this.

Firstly, last Easter, I went to a hospital in Aberdeen where a breast cancer diagnosis tool was being trialled by the NHS Trust there, and it had worked. It had flagged tiny early-stage symptoms of breast cancer in 11 women that the human radiologists had missed. I spoke to one of these women. Many of the women in her family had suffered with breast cancer, but she hadn't suffered because of the swift action that was taken and the fact that it was caught so early. The tool worked because it had been trained on thousands and thousands of anonymised mammograms.

And secondly, a little poem:

A Poem About AI

The AI learns, it's sharp, it's quick,
It sees through every little trick.
Incognito, prohibit mode,
A hollow hope, a winding road.
And yet I like it. Should I not?
It helps a lot. It saves a lot.
It writes my emails, spells things right.
It finds the cheapest holiday flight.

That's a poem about AI and data privacy produced by ChatGPT in the style of one of my favourite poets, Wendy Cope. It’s not as good as she is, I don't think so, but it's not bad, and the reason for that is because it was trained on her work.

The Dilemmas of Patient Data Privacy

Now here are the problems. Because of patient data privacy, there were also a lot of false alarms in the breast cancer trial, and thousands of women took part. The AI tool did not have access to any of the women's previous histories, so it didn't know about benign tissue changes that had already been ruled out in previous scans.

And there's a second postscript to that story. The firm which built the tool has now been acquired, along with all of its data, by a company in the US, and its future here is currently unknown. Is it fair on Wendy Cope that ChatGPT can mimic her so well? Was she asked before her work was scraped to train it? We know that that's not very likely, and this is where legislation, I think, needs to play a role.

Rethinking Data Rules

My advice to you all is that it's time to think differently about data rules in the age of AI. The way in which AI consumes data and developers make money from it is not like the more direct transactions that we've seen with tech firms in the past, like social media and search engines, for example. And unfortunately, I don't think our current data legislation is entirely compatible with the AI space for this reason.

Current Data Principles

We've got some really sound principles which still apply: anonymisation and limiting human access to data at developer level, for example. But once it's been used to train an AI product, it can't be readily erased on demand if somebody wants it to be. There's no defined period of use in terms of how long it might be used for, and there's a lack of transparency around exactly where and how individual data is used. Most AI systems are proprietary, and their owners don't really want to open the hood; believe me, I've asked.

The Future of AI Legislation: Balancing innovation with privacy

So what is the most responsible way to balance AI innovation and growth with data privacy and fairness? I really wish it was something I could tell you about in six minutes, but here are a few possibilities that I think we should explore.

(1) Opt-Out Decisions

The first is the UK making data use for AI purposes an opt-out decision, opening up by default. This is roughly what's being proposed in the current copyright consultation, and it would certainly benefit innovation, but there's strong opposition to it, especially from the creative industries.

(2) Categorising AI Products

The EU AI Act categorises AI products according to how serious they are. Perhaps AI-focused data law could take a similar approach with different rules depending on the data's ultimate purpose. After all, an AI tool can still effectively diagnose cancer without generating poetry.

(3) Prioritising Synthetic Data

Prioritising synthetic data is the second possibility. This is the scenario of AI generating its own training data, and ultimately this does—and probably will—eventually solve the issue for us. But there’s still human-gathered data involved in its development, as well as probably human oversight in ensuring that it's accurate and unbiased, and that all still needs to be lawfully managed.

(4) International Collaboration

Collaboration is another key point. The UK did not sign the AI Action Summit declaration in Paris last month, citing national security concerns. But AI is a global phenomenon, and working with other countries to agree on data standards across borders feels more important than ever. However, it also feels more difficult than ever, as we saw in Paris. I also think everyone’s a bit tired of voluntary codes and guidelines. Collaboration is only going to work if it's both decisive and binding.

(5) Licensing Agreements

The most popular solution that I’ve seen around so far is the idea of a licensing agreement model between AI developers and data owners—perhaps a little bit like the streaming agreements we have now. This would reward data owners for sharing their data with the industry and ultimately also lead to better AI systems as a result. With legislation-led terms of agreement, perhaps this would give everybody more control.

Conclusion

Lots of people that I speak to are in favour of AI and they understand its potential benefits as a useful tool for society. But they also fear not being able to control their data in the race to develop ever more advanced products. I think solid legislation and clear collaborative direction would not only help them to feel more protected, but also lead to better quality data training, better AI models, and that would make the UK an attractive place for AI firms to set up.

Summary of Zoe Kleinman’s Evidence Statement

Key Points

- Role and Expertise: Zoe Kleinman is the technology editor at BBC News. In her role, she focuses on reporting a wide range of technology-related news stories across various BBC platforms, including TV, radio, and digital media. Her expertise lies in technology journalism, with a particular emphasis on topics such as artificial intelligence, data privacy, and the ethical implications of emerging technologies.

- Data Quality in AI: Emphasised that AI tools are only as good as the data they are trained on, highlighting the phrase "garbage in, garbage out." Good data is essential for effective AI performance.

- Real-World Examples: Cited a successful breast cancer diagnosis tool that flagged early-stage symptoms in women, demonstrating the potential of AI when trained on quality data, contrasted with challenges in data privacy.

- Data Privacy Challenges: Raised concerns about false alarms in AI tools due to lack of access to complete patient histories and identified that patient data privacy poses significant dilemmas for AI applications.

- Legislation Needs: Called for updated legislation that reflects the unique challenges posed by AI, arguing that current data laws are not fully compatible with AI's operational requirements.

- Rethinking Data Rules: Advocated for innovative approaches to data use, including making data use for AI purposes an opt-out decision and categorising AI products based on their risk levels.

- Prioritising Synthetic Data: Suggested focusing on synthetic data generation as a long-term solution to data privacy issues while ensuring human oversight to maintain quality and bias prevention.

- International Collaboration: Highlighted the importance of global cooperation in establishing data standards, noting the challenges of achieving effective collaboration.

- Licensing Agreements: Proposed a licensing model for AI developers and data owners, akin to streaming agreements, to incentivise data sharing while protecting rights and encouraging innovation.

- Balancing Innovation and Protection: Stressing that while people see the benefits of AI, they are also wary of losing control over their data, suggesting that solid legislation and collaborative frameworks can help alleviate these concerns.

Actions for Stakeholders

- Engage in Legislative Reform: Stakeholders should advocate for updated data legislation that aligns with AI capabilities and prioritises privacy while fostering innovation.

- Participate in Data Framework Discussions: Engage with policymakers and industry leaders to discuss the development of flexible data frameworks that can accommodate both innovation and protection.

- Support Synthetic Data Initiatives: Explore and invest in synthetic data generation technologies that can provide safer alternatives for training AI while adhering to ethical standards.

- Collaborate Internationally: Work with global partners to establish common standards for AI data usage and privacy that can transcend national boundaries.

- Consider Licensing Models: Evaluate the feasibility of a licensing agreement system for data sharing that balances the interests of data providers and AI developers.

By addressing these key points and taking action on the outlined initiatives, stakeholders can play a crucial role in shaping the future of AI in a responsible and effective manner.

Oliver Patel:

Enterprise AI Governance Lead, AstraZeneca.
AI Governance & Policy Expert.

My name is Oliver Patel. I'm head of enterprise AI governance at AstraZeneca, which is a global pharmaceutical company and the UK's largest company by market cap.

AI Governance Framework

I'm going to be presenting primarily on behalf of AstraZeneca, but I will also let you know when it's my own personal view. I've been at AstraZeneca for about two years now, and in that time, I've been leading the work to develop and implement our global approach to enterprise AI governance, risk management, and regulatory compliance. What we've been doing is putting in place an AI governance framework, which enables AstraZeneca to maximise the value of AI whilst mitigating risks, complying with regulations, and protecting our business and our patients.

Presentation Outline

I'm going to be speaking about three points today in my presentation:

1. How AstraZeneca uses AI and how the global regulations that are coming in, that have come in the EU, in China, and in other markets are impacting our business, along with some takeaways that are relevant for UK legislators.
2. The emerging challenges, risks, and opportunities of agentic AI, which I think we're only just starting to wrap our heads around, especially in terms of privacy, cybersecurity, and AI governance more broadly in the era of agentic AI.
3. A touch upon AI literacy and upskilling, and how important that is to actually addressing the challenge of AI, particularly agentic AI.

I've chosen these topics because I want to bring the debate to life with some real-world examples that are relevant for AstraZeneca and the healthcare and life sciences sector more broadly. I also think that the emergence of agentic AI as the next frontier of AI development and research poses novel risks. There's a great opportunity now for the UK, which hasn't got its own comprehensive AI legislative framework in place yet, to consider what the risks and challenges of agentic AI are and how they can be factored into the policy work.

Revolutionising Work at AstraZeneca

First of all, the field of AI is really revolutionising the way we work at AstraZeneca. There’s no single area that we use AI; we’re using it across the board to accelerate the drug discovery and development process, optimising, enhancing, and speeding up every constituent part of that process. We’ve got about 700 AI and data science practitioners in the organisation, so on a day-to-day basis, it feels more like a tech company than a pharma company. We have 400 to 500 active AI projects.

For a couple of examples, we're using AI to accelerate drug discovery and design, and we even have AI-generated molecules in our pipeline of drugs today. We also use AI to speed up design and optimise clinical trials. For example, to improve the experience and efficacy for researchers and patients alike. We're using AI in that context to improve things like adverse event detection and adjudication. Doing that more efficiently and autonomously can have massive benefits in terms of how long trials take. Ultimately, what we're aiming to do is discover and develop new medicines more quickly so that we can get them to the patients that need them.

Ethical Considerations

When I think about the use of AI, my background is in philosophy and ethics. I spent several years as an academic at University College London, looking at the ethics and governance of AI, and I truly believe that the risks of not adopting AI are greater than the risks of adopting AI. Examples in healthcare, such as the one mentioned in the previous presentation, tell me that we have an ethical duty to look at how we can use these tools for things like earlier detection and diagnosis of cancer. So we're very pro-AI and very positive, but we have obviously put in place an AI governance framework because we're aware of the risks, and we believe in responsible AI.

AI Governance Framework Alignment

We designed and rolled out that framework in alignment with international standards and laws like the EU AI Act and a risk management framework like ISO 42001. However, as we consider agentic AI, I think we’re starting to realise that those frameworks haven’t properly factored in some of the challenges and risks associated with agentic AI.

Personal Views on Agentic AI

Now, this part is my personal view; it’s not necessarily AstraZeneca’s company position. Most traditional AI governance and regulatory frameworks were developed in an era where you mainly had a machine learning model that performed a specific task, trained on a specific dataset. You would monitor the performance of the model in production, checking how well it performed the predefined task. The AI would generate an output or a score or a prediction, and then a human would take that and review it.

However, agentic AI is transforming how AI is developed and deployed. We are moving into a world where AI systems can autonomously develop plans, solve problems, use tools, and execute tasks in a range of applications. A classic example is a holiday booking agent where you input a natural language prompt, such as "Please book me a holiday to Corfu this time of year. I've got this many children and these are my criteria," and it processes all that information. You then have various AI agents or bots working together to decide which systems to connect to, what information to retrieve, and ultimately making a plan and executing it based on your permissions and the parameters you've set.

Challenges of Agentic AI

I don't believe that the current AI governance and regulatory frameworks fully account for the implications of having agents that can make such autonomous decisions. What we see here is an increasing autonomy of AI. AI is no longer merely generating content; it is actively doing things and beginning to genuinely replace tasks that previously required human intervention.

Some of the risks associated with this involve cybersecurity, where you move from AI that merely generates code to AI that generates and executes code. This shift can create cybersecurity vulnerabilities, as there is a possibility of malicious code being executed without oversight or checks in place.

Privacy challenges arise as well; an AI agent may have access to systems or databases that it shouldn’t interact with, leading it to mine sensitive data without proper consent or oversight in executing its tasks.

Human Oversight Challenges

One of the most significant challenges is human oversight. We often talk about the importance of having a "human in the loop," but in the era of agentic AI, this is increasingly unfeasible. The very purpose of agentic AI is to remove the human from the loop and place trust in AI to act on our behalf.

Setting the scene with these challenges illustrates that we are confronted with a slew of risks and challenges that we have not yet fully explored. At the same time, the UK’s somewhat cautious approach to AI regulation presents an opportunity to integrate the unique dimensions and implications of agentic AI into our policymaking processes.

Importance of AI Literacy

Finally, I must highlight the issue of AI literacy. It's already difficult enough for technical leaders and AI governance professionals to keep up with traditional AI and generative AI, let alone understanding agentic AI. The general public and the wider workforce face even greater challenges in keeping pace with these rapid developments.

One positive aspect of the EU AI Act is its focus on AI literacy, which I believe is something the UK should champion and continue to promote. It’s vital that we ensure a breadth of understanding across society about these technologies, their implications, and their responsibilities moving forward.

Conclusion

In conclusion, as we explore the opportunities and challenges that lie ahead with AI, particularly the emergence of agentic AI, we must prioritise a comprehensive governance framework, promote AI literacy, and proactively address risks while harnessing the benefits that AI can offer to health and science.

Summary of Oliver Patel’s Evidence Statement

Key Points

Role and Expertise:

- Oliver Patel is the head of enterprise AI governance at AstraZeneca, a leading global pharmaceutical company.
- He has been instrumental in developing and implementing a global approach to AI governance, risk management, and regulatory compliance.

Implementation of an AI Governance Framework:

- AstraZeneca is utilising an AI governance framework to enhance the value of AI while mitigating risks and ensuring regulatory compliance.
- The framework aligns with international standards to promote responsible AI use.

AI's Role in Drug Discovery:

- AI is widely used within AstraZeneca to accelerate drug discovery and development, employing around 700 AI and data science practitioners.
- The company is focusing on using AI for efficient clinical trials, enhancing patient experiences, and expediting the drug development process.

Ethical Duty in AI Adoption:

- Patel believes that the risks of not adopting AI in healthcare outweigh the risks of its adoption, highlighting ethical responsibilities for earlier detection and diagnosis, such as cancer.

Emergence of Agentic AI:

- Patel discusses the advent of agentic AI, which autonomously develops plans, solves problems, and executes tasks, necessitating a reevaluation of existing governance frameworks.
- Current regulatory frameworks are outdated as they were primarily designed for less autonomous AI applications.

Increased Cybersecurity and Privacy Risks:

- The transition to agentic AI brings new cybersecurity risks, such as the potential for executing malicious code without oversight and unauthorized data access.
- Human oversight becomes increasingly challenging as AI takes more autonomous actions.

AI Literacy Importance:

- Emphasises the need for increased AI literacy among stakeholders, including the general public, to understand AI implications and responsibilities.
- Highlights the focus on AI literacy in the EU AI Act as a model for the UK.

Actions for Stakeholders

Advocate for Proactive AI Governance:

- Stakeholders should engage in discussions to develop an updated governance framework that takes into account the unique challenges posed by agentic AI.

Encourage Responsible AI Adoption:

- Promote and support initiatives that advocate for the ethical use of AI, highlighting the benefits of its adoption in healthcare and other sectors.

Focus on Cybersecurity Measures:

- Emphasise the importance of integrating robust cybersecurity measures in AI development and deployment to mitigate associated risks.

Enhance AI Literacy Programs:

- Champion AI literacy initiatives to ensure that both technical leaders and the general public are well informed about AI technologies and their implications.

Monitor Legislative Developments:

- Stay informed about ongoing legislative discussions and frameworks in AI regulation, ensuring that stakeholder perspectives are represented in policymaking.

By acting on these key points and recommendations, stakeholders can contribute positively to the responsible advancement of AI technologies while addressing associated challenges and risks.

Sunaina Aytan

Cybersecurity Consultant, Airbus Protect
Trustworthy AI Security Specialist

My name is Sunaina Aytan. I'm a cybersecurity consultant at Airbus Protect. Over the last seven years, I have been developing and shaping cybersecurity strategies in both the IT and the OT (operational technology) areas, helping government entities in improving their cybersecurity posture and, more recently, providing consulting services to ensure the delivery of secure and safe AI-based products. I'm also leading up the trustworthy AI initiatives at Airbus Protect, leveraging my experience within the defence and space industry.

AI and Safeguarding National Interests

For this session, I will be presenting a deep dive into the use of AI and safeguarding national interests. Firstly, it’s important to understand that there are two aspects of AI and cybersecurity:

1. AI for Security: How we can leverage AI to improve our cybersecurity.
2. Security of AI: The importance of creating cybersecurity-proof AI solutions.

Leveraging AI for Enhanced Cyber Security

To begin with, I will discuss the ways in which we can leverage AI to enhance cybersecurity measures to protect critical infrastructure. AI technologies can automate the detection of threats and vulnerabilities by analysing vast amounts of data in real time, allowing for quicker responses to potential breaches and improving incident response time. Currently, we are relying on human analysts working 24/7 to understand whether threats are happening.

Predictive maintenance powered by AI can also ensure that critical infrastructure such as power grids and water supply systems remain resilient against cyber threats by identifying weaknesses before they can be exploited. This technology enables businesses to refine their disaster recovery strategies based on predictive analysis, which is vital for maintaining integrity and resilience.

Currently, many key businesses in the UK are still struggling to understand what a disaster strategy or incident response plan actually looks like because they don’t fully grasp the scope of potential threats to their business.

Digital Twin Technology for Operational Technology

So far, I have discussed AI use cases for IT and critical infrastructure, but for operational technology (OT), there's a key use case in the use of a digital twin. A digital twin is a virtual model of a physical system, complemented by an AI-powered counterpart. An example of critical OT (operational technology) infrastructure is a power plant. A digital twin can be used to simulate the effects of a crisis and proactively address potential threats before they can impact the physical system. This is a threat-based scenario solution where we can experiment to understand potential outcomes in critical infrastructure.

AI Advancements and Risks

As AI advancements continue to shape cybersecurity use cases, it is critical to highlight the potential risks that may arise in the process. If I were to ask the audience if they would sit in a self-driving car that hasn't been safety tested, I'm sure the answer would be no. Yet, we continue to create and use AI technology without fully understanding the significance of cybersecurity.

One area of concern that we should be addressing is the potential use of commercial AI systems by malicious actors. For instance, the use of drones or autonomous vehicles to carry out explosive attacks or cause serious accidents. As these physical objects become increasingly digital, it is crucial to consider their security implications alongside their safety.

Airbus Protect's Responsibility

As an entity of Airbus, our major goal is to deliver passengers safely and securely, but we now have additional objectives because our planes are becoming more digital and we do not have cybersecurity specialists on board to assist in case of any such attack.

A research project conducted by the Royal United Services Institute on behalf of GCHQ (Government Communications Headquarters) found that AI will transform what were previously classified as high-skill attacks into tasks that low-skill attackers can perform with little effort. This means that attackers no longer need the same skill set as before to create sophisticated attacks.

The increased adoption of Internet of Things technology and interconnected critical national infrastructure, which will now also include agentic AI, will create numerous new vulnerabilities that could be exploited by threat actors to cause damage or disruption.

Changing Organisational Culture

Critical infrastructure operators face far more constraints than organisations in other industries and therefore must be extra cautious about disclosing information about their systems. To mitigate these risks, it is important to change the mindset of organisational culture within critical infrastructure environments and to prioritise cyber risk as seriously as you would safety risk.

Risk management should be integrated into enterprise risk management. To address AI risk properly, it must be fully integrated into existing enterprise risk management practices, and this should be discussed at top management level. Key standards and frameworks such as the NIST Risk Management Framework and ISO 42001 should be taken into consideration when managing these AI environments.

Technical Perspective on AI Integration

From a more technical perspective, when adopting or developing AI technology, it is essential to engage in transparency. Publishing information about models in formal model cards provides trust and explainability. Conducting thorough security testing and threat-based simulations is integral to ensuring security robustness within the supply chain and the entire organisation.

Continuous monitoring and auditing are essential to maintaining the integrity of AI systems. Regular assessments can help identify anomalies and potential threats before they escalate. This proactive approach ensures that any vulnerabilities are addressed in a timely manner, thereby reducing the risk of breaches. Establishing a routine for monitoring the full performance and security of AI systems is vital in sustaining robust cybersecurity practices.

Collaboration Between Governments and Industries

So how can governments and industries collaborate to address the evolving landscape of cyber threats? We need to harmonise regulations relevant to securing AI systems and data privacy. The understanding of what these regulations mean needs to be simplified and made meaningful, especially for small and medium enterprises (SMEs) that may lack the budget or expertise to comprehend cyber threats in relation to AI.

The silos between government and industry must be broken down. Instead of working in parallel, we should be working in tandem. Developing guidance that applies to everyone runs the risk of fitting no one. The government needs to collaborate with sector partners to tailor and operationalise guidance specific to each sector, which is critically important when discussing critical infrastructure.

Importance of Information Sharing

A culture that prioritises information sharing between government and industry is needed to understand potential security risks in real-time. Currently, we lack a proper information-sharing regulation or model that allows sectors and government to see what types of threats organisations and industries are facing. This information should be widespread knowledge, yet the current culture often leans towards “name and shame.” If a cyber incident occurs, organisations may hesitate to disclose it until absolutely necessary, and if it falls outside GDPR, it may never be known.

The UK’s Opportunity in AI Regulation

I believe that the UK is in a sweet spot concerning our approach to AI regulation when compared to Europe and the rest of the world. Europe has extremely stringent regulations, while in the United States, regulations are fragmented at the federal and state levels. There is uncertainty about what the current government will do.

If we can establish a strong foundation for AI security—something that most other regulations do not focus on—I believe that the transition of the AI Safety Institute to the AI Security Institute is a step in the right direction. There’s an ongoing discussion about whether to adopt this change, but it's clear that AI security must encompass AI safety, while AI safety does not inherently cover AI security.

If we can successfully align our regulations and foster an environment that promotes AI innovation in a secure, trustworthy, and explainable manner, without hindering innovation or raising barriers to entry, then the UK could lead in AI regulation. That is our aim.

Conclusion

To sum up, as AI continues to evolve and become integrated into various systems, the importance of robust cybersecurity measures cannot be overstated. By addressing the risks associated with AI, focusing on effective collaboration between government and industry, and promoting a culture of information sharing and transparency, we can work toward safe and innovative AI solutions that protect national interests.

Summary of Sunaina Aytan's Evidence Statement

Key Points

Role and Expertise:

- Sunaina Aytan is a cyber security consultant at Airbus Protect, with over seven years of experience in developing cybersecurity strategies for both IT and operational technology (OT) sectors, particularly in the defence and space industry.

AI in Cybersecurity:

- AI can enhance cybersecurity measures by automating the detection of threats and vulnerabilities, improving incident response times, and supporting predictive maintenance to protect critical infrastructure.

Digital Twin Technology:

- The use of digital twins—a virtual model with an AI counterpart—can simulate crises in critical OT (operational technology) infrastructure, allowing for proactive threat assessment and mitigation before impacts occur.

Risks Associated with AI:

- As AI technology is adopted, there are potential security risks, including the misuse of commercial AI by malicious actors, such as using drones for attacks. The implications of digital transformation in physical objects (e.g., aircraft) need to be addressed.

Evolving Skill Requirements:

- AI may lower the skill barrier for attackers, transforming high-skill attacks into tasks manageable by low-skill individuals, raising significant concerns for cybersecurity.

Cultural Change in Cyber Risk Management:

- Critical infrastructure operators must integrate cyber risk management into enterprise risk management, prioritising it on the same level as safety risk.

Importance of Transparency and Monitoring:

- Emphasised the need for transparency in AI models, rigorous security testing, and continuous monitoring to maintain the integrity of AI systems.

Collaboration Between Governments and Industry:

- Highlighted the need for governments and industries to harmonise regulations related to AI systems and data privacy, facilitating meaningful guidance tailored for various sectors, especially for SMEs.

Information Sharing:

- Stressed the importance of creating an effective information-sharing model between government and industry to address potential cybersecurity threats in real-time.

UK's Regulatory Landscape:

- Positioned the UK as having an opportunity to lead in AI regulation by focusing on AI security, contrasting it with stringent European regulations and the fragmented U.S. approach.

Actions for Stakeholders

Promote a Culture of Cyber Awareness:

- Encourage the prioritisation of cybersecurity as a core organisational value and integrate it into enterprise risk management strategies.

Enhance AI Governance Frameworks:

- Develop and implement governance frameworks that incorporate both security and safety aspects of AI technologies to foster responsible innovation.

Facilitate Collaboration:

- Advocate for stronger collaboration between government entities and industry sectors to create tailored, applicable guidelines for managing cybersecurity risks.

Invest in Transparency Initiatives:

- Support initiatives that focus on transparency in AI models, including the publication of formal model cards and conducting security testing.

Establish Information Sharing Mechanisms:

- Work towards establishing robust information-sharing frameworks that facilitate timely communication about cyber threats and incidents between sectors and government.

Educate and Upskill:

- Promote education and training initiatives aimed at improving understanding of AI risks and cybersecurity practices among all organisational levels, particularly in smaller enterprises.

Monitor Regulatory Developments:

- Stay engaged with regulatory changes and advocate for policies that balance innovation with the necessary security measures to mitigate risks associated with AI.

By focusing on these key points and actions, stakeholders can help enhance the security and resilience of AI systems while fostering a culture of innovation and responsibility.

Ben Johnson

Co-Founder & Chief Technology Officer, Uptitude

My name is Ben Johnson, and at Uptitude, we help enterprises solve data and AI challenges while supporting the adoption of AI technologies, collaboration, and cybersecurity awareness. We believe best practices should be shared openly, as they represent a non-competitive behaviour essential for uniting against a common threat: cybercriminals and hostile foreign actors.

Individual Rights Management and Data Privacy

I'm going to mention two points—one about individual rights management and one about cybersecurity in AI. Organisations want our data; they want our data to provide a better service, more stable experiences which are much better for us. They want to save our time, reduce the price of products and services. Pharmaceuticals want our data so they can improve medicine and medical devices. The collection of personal data is increasingly valuable.

But there are others who do not have positive intentions, who want to collect our data for less favourable reasons; they seek to defraud us. Organisations that fail to maintain the privacy of individual data face fines and loss of trust, which can be hard to recover from. The response to protecting that data should be relative to the increase in the value of the data. There should be a corresponding increase in investment to stay one step ahead of bad actors.

Human Factors in Cybersecurity

Beyond software and systems, I believe humans will continue to be the weakest link. Social engineering cyber attacks will become more sophisticated, enhanced with AI, and even more effective in the near future. Employees and civil servants will not receive bulk-generated phishing emails, but complex AI-generated content that is hyper-personalised to them.

It will contain information from social media, LinkedIn, and personal details from recent events. They will start to receive deep fake audio and video from colleagues and senior colleagues with simple requests that may be impossible to differentiate from the real thing. Anyone who has ever posted audio or video of themselves on social media may have already provided enough of a digital signature to make this possible.

Editor’s note: Social engineering is a manipulative tactic used by cybercriminals to deceive individuals into revealing confidential information. It exploits human psychology rather than relying on technical hacking methods. Common techniques include:

1. Phishing: Fraudulent emails that appear legitimate to trick recipients into sharing sensitive information.
2. Pretexting: Fabricating a scenario to pose as someone else and obtain private information.
3. Baiting: Offering enticing items (like free downloads) to lure targets into revealing information or installing malware.
4. Spear Phishing: Customised phishing attacks targeting specific individuals or organisations.
5. Tailgating: Gaining physical access to restricted areas by following someone who has legitimate access.
6. Vishing: Using phone calls to trick individuals into providing personal information.

As social engineering attacks become more sophisticated, especially with AI, it's essential for people and organisations to be educated and vigilant against these threats.

Increased Threat of Blackmail

The personal side of blackmail is also likely to increase, leading to professional consequences for workers who feel scared or trapped. People need to know how to detect these new threats and how to react to them, both in professional and personal settings. Training should address this personal side, as it’s unlikely they will receive this type of training outside of the professional environment, making it important for businesses and organisations to address.

Evolving AI Landscape and Training

The AI landscape is evolving faster than ever, and so must our approach to training. Traditional once-a-year blanket training should be augmented with more targeted and risk-based campaigns. More efficient training is more engaging and will result in higher levels of retention. Action using generative AI learning scenarios can be custom-generated to closely mimic specific individual work scenarios, making everything more relatable.

We can use conversational responses to questions which can replace the standard A, B, C, D type responses.

Data Sharing for the Greater Good

The next point is about sharing data. Sharing individual personal data, as we've heard, can be used for the greater good, one of the most obvious being the sharing of medical or clinical trials data with AI. We can analyse more and more data to better understand how humans react differently to drugs, treatments, and environments.

However, too often, the conversation and narrative around AI and privacy revolves around the negatives and the risks. A sentiment that is overly punitive may lead to overregulation or individuals choosing not to share their personal data or opting out. It is crucial to have equal voices, both positive and negative, to make informed decisions.

We need more hero stories about AI. At the last APPG AI meeting [AI & Government: AI in the Public Sector – Redefining Government & Welfare with AI held on 20 January 2025], I was touched to hear about the real impact AI was having on caseworkers and how they can deliver unprecedented levels of care by automating low-complexity paperwork. With AI, we could produce GP appointment waiting times from 10 days to 10 minutes. With AI, we might reverse climate change—not in our children's lifetimes, but in our own. These are the kinds of hero stories I think we need to hear more of.

Closing Remarks

In my closing remarks, I believe we need to focus more on how training can be used to detect social engineering attacks as generative AI and deepfakes become standard technology for criminals. Training should be delivered as often as required to keep up with the pace of change, which may be sooner than once per year. Training and testing should be enhanced with generative AI to be more targeted, engaging, and therefore effective.

Lastly, I hope we can support the positive sentiment about the benefits of AI and remind the public of the advantages of sharing their individual data for the greater good, which in my opinion far outweigh the risks.

Summary of Ben Johnson’s Evidence Statement

Key Points

Role of Altitude:

- Ben Johnson is the Co-Founder and CTO of Uptitude, where he helps enterprises address data and AI challenges while driving the adoption of AI and fostering collaboration to strengthen cybersecurity efforts.

Need for Collaboration Against Common Threats:

- Emphasises that cybersecurity best practices should be considered non-competitive and focused on combating common threats from criminals and foreign bad actors.

Data Value and Risks:

- Organisations collect personal data to enhance services and customer experiences, but there are risks from malicious actors seeking to defraud individuals.
- Failing to protect this data can lead to fines and loss of trust, which are difficult to recover from.

Weakness of Human Factors:

- Highlights that humans remain the weakest link in cybersecurity. Social engineering attacks will become more sophisticated with AI-generated, hyper-personalised threats.

Training on Emerging Threats:

- Stresses the need for ongoing training to help individuals recognise and respond to new threats, including deep fakes and complex phishing attempts, both in personal and professional contexts.

Evolving Training Methods:

- Advocates for a shift from traditional blanket training to targeted, risk-based training that is more engaging and effective, utilising generative AI to create relatable scenarios.

Positive Data Sharing:

- Acknowledges that sharing personal data, especially in medical contexts, can significantly benefit society but highlights the need for balance in the conversation around AI privacy to avoid overregulation.

Promoting Positive AI Narratives:

- Calls for more positive stories about AI to highlight its benefits, such as improving healthcare efficiency and addressing climate change.

Actions for Stakeholders

Cultivate Collaborative Approaches:

- Encourage organisations to adopt a collaborative mindset in sharing cybersecurity best practices to combat common threats effectively.

Invest in Data Protection:

- Stakeholders should prioritise investments in data protection to avoid fines and loss of trust, ensuring that data privacy measures are proportional to the value of the data.

Implement Enhanced Training Programs:

- Develop and implement training programs that are frequent, targeted, and engaging to keep employees informed about emerging cybersecurity threats and response strategies.

Utilise Generative AI for Training:

- Incorporate generative AI into training scenarios to create realistic, relatable examples that improve retention and understanding of cybersecurity practices.

Promote Positive Aspects of Data Sharing:

- Advocate for the benefits of sharing personal data for the greater good, particularly in areas such as healthcare, to counterbalance the narrative focused on risks.

Foster Positive AI Narratives:

- Work towards increasing public awareness and understanding of the positive impacts of AI, encouraging the sharing of success stories that highlight its benefits.

By focusing on these points and actions, stakeholders can enhance their cybersecurity strategies while promoting a balanced understanding of AI's potential benefits and risks.

Saj Huq

Chief Commercial Officer, Plexal
Member, National Cyber Advisory Board

My name is Saj Huq. I'm Chief Commercial Officer at Plexal. We're an innovation and growth company that specialises in government innovation. For the last seven years, we've played a key role in helping to develop the UK cybersecurity ecosystem, and we also work with national security and defence agencies to build new technologies, drive economic growth, and enhance our national resilience.

The Convergence of AI and National Security

My role focuses on overseeing our work in the cyber and national security space. I want to talk to you about the increasing convergence between AI and national security. First of all, why should governments and industry collaborate in this area? I don't think it's an option; it's a necessity. I will also outline why I believe the UK is well-placed to play a leading role in this respect and provide a few examples.

In terms of the convergence between AI and national security, there is a lot of focus on significant risks associated with the most capable and scaled AI systems. It is important to note that this space is moving incredibly fast. This rapid evolution makes it extremely difficult for any single entity or government to keep up with developments. Many of these capabilities are driven by large amounts of private sector investment occurring outside of governments—not just in the UK, but globally.

Opportunities and Concerns

The convergence of these factors stands to drive both substantial benefits and serious concerns. I don't need to elaborate on the risks we have already discussed. However, I believe the UK is well-positioned to benefit from some of these developments, and we are already active in this space.

The Necessity of Collaboration

Why should governments and industry collaborate? From an adversarial perspective, there is increasing hybrid integration between public and private interests in cyberspace. We have observed this over the last few years, with alignment between state actors and non-state actors regarding mutual interests. For instance, the rise of ransomware often serves dual purposes: raising funds for nation-states and conducting cyber operations with plausible deniability.

This convergence on the offensive side of the adversary spectrum underscores the imperative for public-private collaboration in cybersecurity. The UK has taken significant steps in this direction. Back in 2016, the UK government released its second of what has now been three cyber strategies, emphasising the importance of national security interests in cyberspace while fostering economic growth. There is a symbiosis between economic development and national resilience; a more prosperous nation is inherently more secure.

Establishing the National Cyber Security Centre

Our cyber strategy over the last couple of years has sought to pursue both goals. In 2016, we established the National Cyber Security Centre (NCSC) as a public-facing arm of GCHQ (Government Communications Headquarters), which provides the benefits and insights of the UK's largest intelligence agency while engaging with industry. Industry needs guidance and support from the government to navigate this evolving cyberspace, particularly as they undergo digital transformation. AI accelerates this transformation, requiring us to double down on our efforts.

The NCSC has already released secure principles regarding AI systems, offering guidance that enterprises need to consider when adopting AI. Additionally, targeted guidance has been created for aspects of the AI development value chain, like software development, to help create technology more securely from the onset.

Research Ecosystem and Economic Integration

The UK is fortunate to have a world-class research ecosystem, with leading AI research happening here, albeit not at the scale of other global players. However, the density of research is significant enough to make a notable impact. Ensuring that this research informs government policy and aligns with industry capability development is vital.

I mentioned the integration between the economy and security—this principle remains significant. AI presents an opportunity for economic transformation and growth that we must not overlook. Driving adoption is critical, and integration between private sector activities and government policy is essential.

Editor's note: The UK government has published three major National Cyber Security Strategies to date, each outlining its approach to safeguarding national interests in cyberspace.

Each strategy built upon the last — moving from foundational capabilities (2011), to operational strength and economic synergy (2016), to strategic advantage and resilience in an increasingly contested cyberspace (2022).

2011–2016 Strategy: This inaugural strategy aimed to make the UK one of the most secure places to do business online, enhance resilience to cyber attacks, and build cybersecurity knowledge and skills.

2016–2021 Strategy: Building upon the first, this strategy introduced the establishment of the National Cyber Security Centre (NCSC) and emphasised defending against cyber threats, deterring adversaries, and developing the UK's cyber capabilities.

2022 Strategy: The most recent strategy focuses on a "whole-of-society" approach, integrating cybersecurity across all sectors and emphasising the UK's leadership in setting global cyber norms and standards.

For comprehensive details on each strategy, you can visit the official UK government publications.

An Overview of those strategies are provided on the next page:

Editor's table:

Strategy	**2011–2016**	**2016–2021**	**2022–Present**
Title	The UK Cyber Security Strategy 2011–2016	National Cyber Security Strategy 2016–2021	National Cyber Strategy 2022
Focus	Laying the groundwork for cyber resilience	Defending UK cyberspace and growing the cyber economy	Whole-of-society resilience and global leadership
Key Institutions	Cabinet Office, GCHQ (Government Communications Headquarters)	Creation of National Cyber Security Centre (NCSC) under GCHQ	Expansion of NCSC role, enhanced collaboration across sectors
Investment	Initial funding for capability building	£1.9 billion National Cyber Security Programme	£2.6 billion cyber programme as part of wider National Cyber Security Strategy
Main Objectives	- Protect UK interests online - Raise cyber awareness and skills	- Defend against threats - Deter adversaries - Develop capabilities - International action	- Strengthen public-private cooperation - Tackle ransomware - Lead in global cyber norms
Economic Link	Promoting safe online business environment	Enhancing UK's position as a secure digital economy	Supporting innovation and cyber industry growth
Notable Firsts	First formal UK cyber strategy	NCSC launched; stronger state-cyber threat posture	Emphasis on "cyber power" and sovereignty in digital infrastructure
International Engagement	Early promotion of cyber norms and diplomacy	Strengthening alliances, e.g. NATO, Five Eyes (USA, UK, Canada, Australia, and NZ) in cyberspace	Deepening international influence in cyber governance and regulation
Cybercrime Focus	Start of cybercrime awareness and legal framework development	Stronger response to cybercrime and state-sponsored actors	Greater emphasis on ransomware, cyber-crime disruption, and law enforcement capabilities

Importance of Insight Sharing

From a national security perspective, collaboration entails greater access and insight sharing between public and private sectors. This requires opening institutions and agencies that historically haven't engaged in this way. Fortunately, this is already happening. Institutions like the NCSC exemplify this trend, as they work more openly with the innovation ecosystem to share challenges and problems at lower classification levels, encouraging new innovations to contribute to the agenda.

Example of Collaboration

Last November, at the NATO Cyber Conference, Pat McFadden, the Chancellor of the Duchy of Lancaster, announced the laboratory for AI Security Research. This collaboration involves multiple government departments due to the cross-cutting nature of the issue. It includes the Foreign Commonwealth Development Office, the National Cyber Security Centre, GCHQ, the Department for Science, Innovation and Technology, and the AI Security Institute, alongside partners like Oxford University and the Alan Turing Institute.

This initiative focuses on conducting world-class research to help the UK shape a secure AI ecosystem globally, investigating both the threats to AI and the threats from AI.

Recommendations for Future Collaboration

This new project exemplifies how public-private collaboration is being designed from the beginning. It is crucial for industry support in this endeavour. I hope to see forthcoming legislative announcements and spending reviews, such as those surrounding defence reform, encourage more diversification within the innovation ecosystem and foster collaboration between public interests and private sector development.

It is essential that we continue to push for these developments, as they are critical in enhancing UK resilience. Our adversaries are actively collaborating and exploiting these opportunities, so we must similarly support our defensive strategies through cooperation and innovation.

Conclusion

In conclusion, the increasing convergence of AI with national security presents both challenges and opportunities. By fostering collaboration between the public and private sectors, leveraging our strong research ecosystem, and ensuring that we integrate economic development with national security, the UK can play a leading role in building a secure AI future.

Summary of Saj Huq's Evidence Statement

Key Points

Role at Plexal:

- Saj Huq is the Chief Commercial Officer at Plexal, an innovation and growth company specialising in government innovation and the UK cybersecurity ecosystem.

AI and National Security Convergence:

- Emphasised the increasing convergence between AI and national security, highlighting the necessity for collaboration between government and industry.

Rapid Development of AI and Cyber Threats:

- Noted the fast-paced changes in technology, which create challenges for any single entity to keep up with developments driven by substantial private sector investment.

Public-Private Hybrid Integration:

- Discussed the hybrid integration of public and private interests in cyberspace, particularly regarding adversarial operations such as ransomware, which often serves both state and non-state actors.

Importance of Cybersecurity Strategies:

- Highlighted the UK's proactive approach since 2016, with the cyber strategy focusing on balancing national security interests with economic growth and resilience.

Establishment of the Cyber Security Centre:

- Mentioned the establishment of the National Cyber Security Centre (NCSC) to engage industry and provide guidance on cybersecurity practices and AI adoption.

Research Ecosystem Strength:

- Acknowledged the UK's world-class research ecosystem and the importance of integrating research insights into government policy and industry capabilities.

Collaboration Initiatives:

- Cited the creation of the laboratory for AI Security Research as a key collaborative effort involving multiple government departments and research institutions to enhance the secure AI ecosystem.

Need for Ongoing Collaboration:

- Urged for continued public-private collaboration to adapt to emerging threats and improve UK resilience in cybersecurity.

Actions for Stakeholders

Foster Public-Private Collaboration:

- Encourage close cooperation between government entities and the private sector to tackle security challenges effectively.

Support Cybersecurity Strategies:

- Stakeholders should align their activities with the UK cyber strategy to ensure a cohesive approach to cybersecurity and national resilience.

Engage with the NCSC:

- Participate in initiatives led by the National Cyber Security Centre (NCSC) to benefit from publicly available guidance and collaborate on cybersecurity best practices.

Leverage Research Collaborations:

- Utilise insights from the UK's strong research ecosystem to inform policymaking and drive innovation in AI and cybersecurity.

Contribute to Collaborative Initiatives:

- Get involved in initiatives like the laboratory for AI Security Research to contribute to world-class research and the development of a secure AI ecosystem.

Advocate for Policy Support:

- Support legislative frameworks and spending reviews that promote innovation and collaboration between public and private sectors in cybersecurity.

By acting on these key points and recommendations, stakeholders can enhance their contributions to a more secure AI environment while fostering collaboration and resilience in the UK cybersecurity landscape.

BIOs of Evidence Givers

Zoe Kleinman
Technology Editor at BBC News
Senior On-Air Journalist | Presenter | Thought Leader

As the Technology Editor at BBC News, Zoe Kleinman brings nearly 20 years of experience in breaking tech news, writing original features, and delivering in-depth analysis across BBC TV, radio, and digital platforms. Her coverage spans AI, robotics, cybersecurity, social media, regulation, and policy, with a focus on making complex tech stories accessible to a large mainstream global audience.

As a senior on-air journalist and presenter, Zoe regularly appears on the BBC’s flagship news programmes. Passionate about gadgets and innovation, she enjoys exploring new products and concepts. She also contributes to the BBC’s tech-focused social media presence, including TikTok and YouTube reports, and uses web analytics tools to enhance online engagement.

Dr Oliver Patel
Enterprise AI Governance Lead, AstraZeneca
AI Governance & Policy Expert

Dr Oliver Patel is an AI governance leader with a decade of experience at the intersection of responsible AI, data privacy, and digital technology policy. He leads the Global Enterprise AI Governance team at AstraZeneca, a multinational pharmaceutical company with over 80,000 employees and a deep AI ecosystem.

A passionate advocate for the safe, trustworthy, and responsible development of AI, Dr Patel serves as a bridge between technical and non-technical domains, ensuring effective communication and implementation of AI governance strategies.

He is a member of the International Association of Privacy Professionals (IAPP) Advisory Board and the OECD Expert Group on AI Risk and Accountability.

Beyond his corporate leadership, Dr Patel has a strong background in academia and research from University College London (UCL), as well as experience in public policy and digital diplomacy for the UK Government. He is also a recognised media commentator and political analyst, having appeared on BBC, Sky News, and CNN.

Sunaina Aytan
Cybersecurity Consultant, Airbus Protect
Trustworthy AI Security Specialist

Sunaina Aytan is a cybersecurity consultant at Airbus Protect, specialising in trustworthy AI security. With extensive experience in the cybersecurity industry, she is committed to strengthening digital resilience and ensuring the security of emerging technologies.

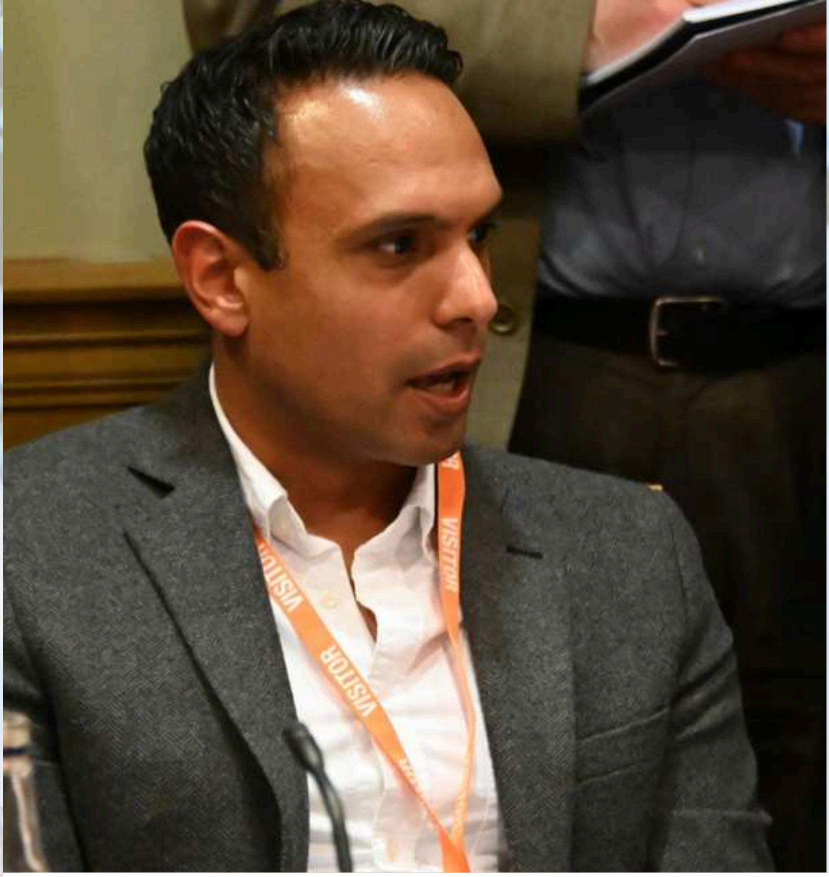
She is a member of the UK Cyber Security Council and serves on the Advisory Board for Cyber London, contributing her expertise to the advancement of cybersecurity policies and best practices.

Passionate about diversity in STEM, Sunaina actively advocates for greater female representation in the field. She collaborates with organisations such as Stemettes and dedicates her time to speaking at webinars, panels, and events to address gender diversity challenges in cybersecurity.

Ben Johnson
Co-Founder & Chief Technology Officer, Uptitude

Ben Johnson is the Co-Founder and Chief Technology Officer of Uptitude, driven by a passion for harnessing AI to enhance work efficiency. With a background in Physics specialising in Quantum Computing, he brings over 15 years of experience in data strategy, rapid software development, and digital transformation across industries including Defence, Pharmaceuticals, Healthcare, Consumer Goods, and Consulting within global corporations.

Ben excels at connecting people with data, simplifying complex concepts, and solving intricate data challenges. His mission is to leverage AI's power to unlock deep insights, accelerate software development, and drive efficiencies in the UK economy. He believes AI can be a force for good, enabling greater productivity while freeing up resources for education and healthcare.



Saj Huq
Chief Commercial Officer, Plexal
Member, National Cyber Advisory Board

Saj Huq is a leading innovation strategist with expertise in cybersecurity, defence, and emerging technologies. As Chief Commercial Officer (CCO) at Plexal, he drives innovation strategy, market growth, and strategic partnerships, collaborating closely with UK government bodies, including the National Cyber Security Centre and the Department for Science, Innovation and Technology.

As a member of the National Cyber Advisory Board, Saj advises on cyber strategy and innovation ecosystems. Previously, as Director of LORCA, he supported 72 cyber startups, helping them secure over £40M in investment and creating 2,000+ jobs.

With a global career spanning Europe, the US, Asia, and the Middle East, Saj has worked with startups, scale-ups, and venture capital firms to accelerate growth. He holds a degree in Aerospace Engineering from the University of Sheffield and credentials from Saïd Business School, Oxford, solidifying his reputation as a recognised leader in cybersecurity and tech innovation.

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

.AI 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

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!

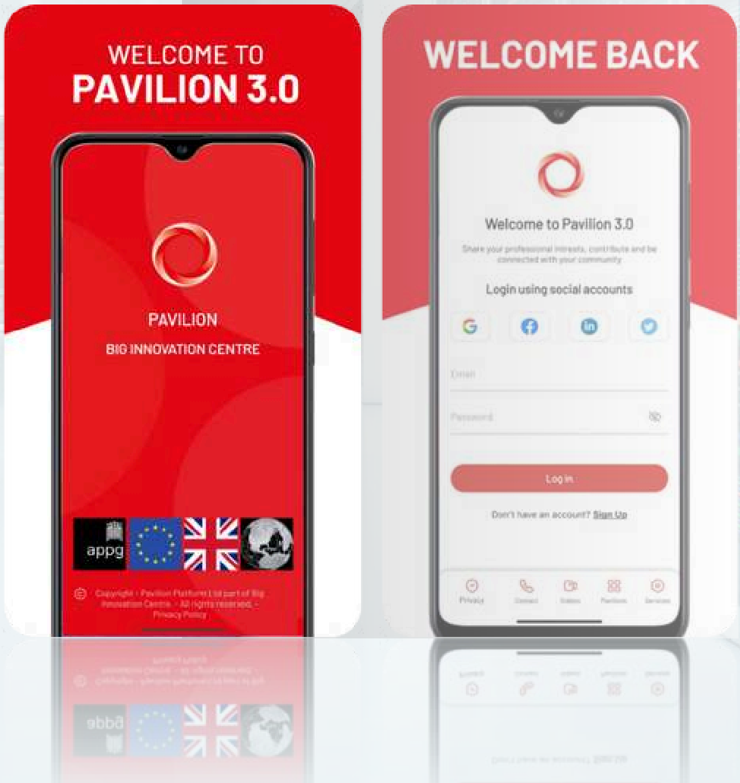
Go to APPG AI Pavilion and click on what you are looking for.

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

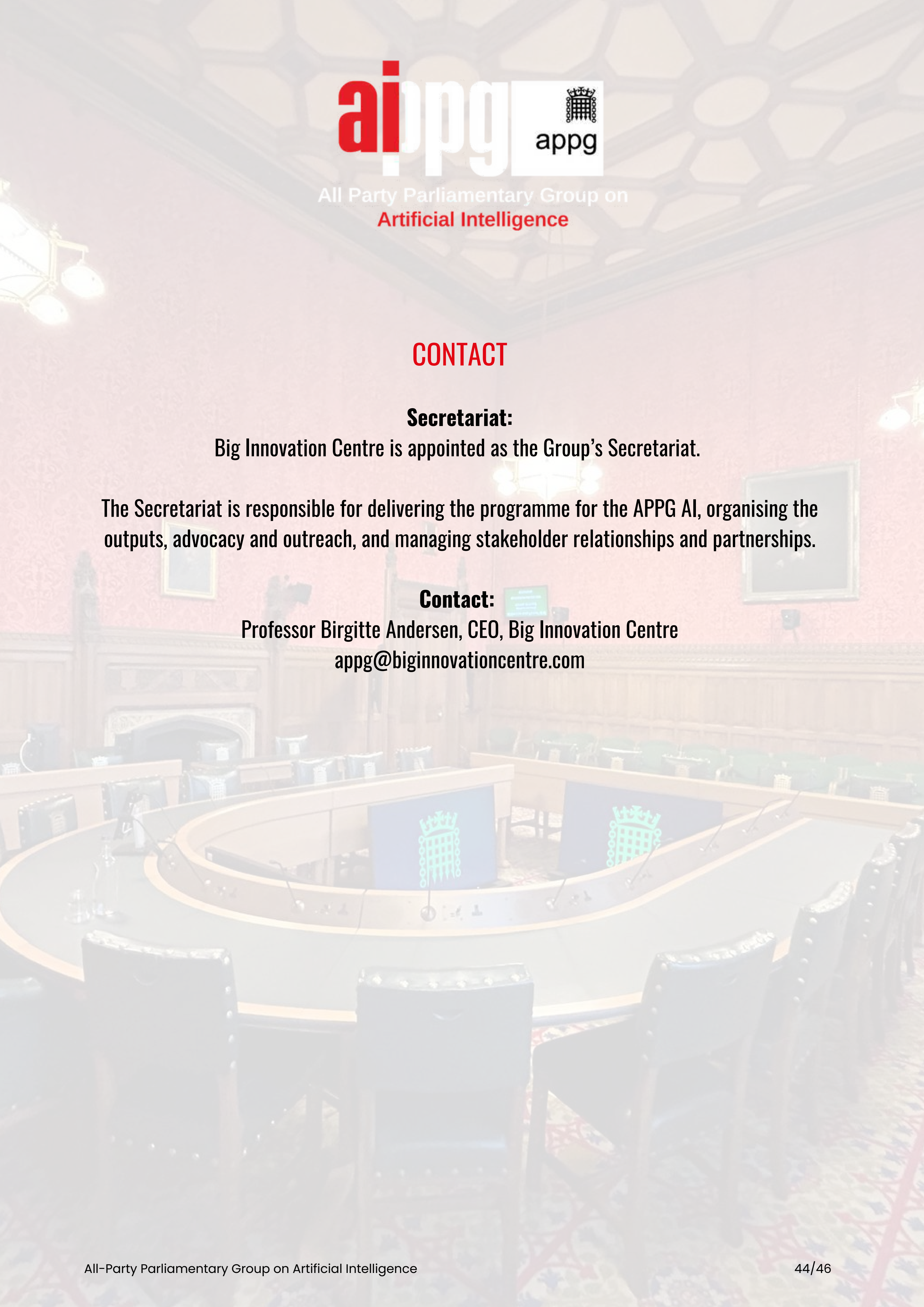


Please use the same username and password across all web and mobile app devices, avoiding the hassle of multiple accounts.
Click below:

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

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.