

Opening Statement
Oireachtas Joint Committee on Artificial Intelligence
6 October 2026
David Hickton

Good morning Chair and Members of the Committee, and thank you for the invitation to appear before you today.

I am David Hickton. From 2010 to 2016, I served as United States Attorney for the Western District of Pennsylvania, appointed by President Barack Obama and confirmed by the United States Senate. As the chief federal law enforcement officer for the district, cybersecurity and cybercrime became a significant part of my work, including cases involving state-sponsored actors and major transnational cybercrime.

In 2014, our office brought the first criminal indictments of identified members of China's People's Liberation Army for hacking American companies to steal intellectual property. Within weeks, we also indicted one of the world's most prominent Russian cybercriminals. Those cases gave me a very direct view of how quickly cyber threats can evolve and how difficult it is for institutions to respond after those threats have become established.

In 2017, I founded Pitt Cyber, an interdisciplinary academic think tank to formulate policy as we sit at the intersection of rapidly changing technology and slow-moving norms, conventions, and laws. Our work has ranged from youth education and workforce development to election security, disinformation, artificial intelligence and decision-making algorithms.

My work in Ireland has developed through a number of closely connected relationships. I hold a Visiting Professorship at Trinity College Dublin's School of Law, and Pitt Cyber has developed a partnership with the Research Ireland ADAPT Centre at Trinity focused on the safe and ethical use of AI. That work connects with the Trinity Centre for Digital Security and Societal Resilience and with Cyber Citizens, a national initiative led by the UCD Centre for Cyber Resilience Education, in partnership with ADAPT at Trinity, Oide Technology in Education, Webwise and Pitt Cyber, with support from the Research Ireland Discover Programme.

Cyber Citizens includes two interconnected strands: Cyber Sense, working with schools, families and libraries, and Cyber Smart for Public Leadership, which I co-lead and which focuses specifically on elected representatives and public officials and on responsible AI, cyber resilience and digital trust.

There are many issues I would welcome the opportunity to discuss with the Committee, but today I want to focus on three. Across all three, my central concern is resilience — whether our citizens, communities and public institutions are equipped to anticipate change, respond to harm and maintain trust as AI develops.

First, we need to protect the most vulnerable.

AI is changing the scale, speed and sophistication of fraud. We need civic resilience, practical skills and general awareness, particularly among those most often targeted. Trusted organisations such as schools, libraries, youth services and community groups should be recognised as part of the wider infrastructure of cyber resilience and equipped to play that role.

But education alone will not be enough. Expecting individuals to be the primary line of defence against transnational criminal enterprises using cloned voices, deepfakes and personalised phishing is unrealistic. Effective protection also requires institutional intervention and appropriate safeguards.

The same principle applies to public leadership. Public leaders do not need to become technical experts, but they do need enough understanding to ask the right questions, recognise risk, understand where responsibility lies and know when specialist advice is needed. Building that confidence is itself part of institutional resilience.

Second, we need to think differently about access and inequality.

For years, we thought of the digital divide largely in terms of access to devices and broadband. Those still matter, but increasingly so do the skills to use AI effectively and access to high-quality tools. There is a real risk that those with the skills and resources to use AI will compound their advantages while individuals, communities, smaller organisations and local governments without those capabilities fall further behind. AI literacy therefore needs to be part of the wider digital inclusion agenda.

Third, we need to prepare for workforce disruption.

I come from Pittsburgh, a region that lost much of its steel industry in the 1980s and still feels the consequences today. AI may bring change across many sectors simultaneously and at much greater speed.

The reality is that you cannot manage what you do not measure. Ireland has an opportunity now to build the evidence needed to understand AI's impact on jobs, entry-level roles, wages and skills, and to invest in upskilling and retraining before displacement occurs rather than after.

Across all three areas, one lesson from the American experience is that we have too often waited for harms to become visible before responding. Ireland does not have to do the same.

With the work of this Committee and Ireland's Presidency of the Council of the European Union, Ireland has an opportunity to show that governing AI well means looking beyond the technology itself to the people and institutions it affects.

Our work through the Trinity Centre for Digital Security and Societal Resilience and Cyber Citizens are practical contributions to that effort. We want to bring together young people, families, communities, researchers and public leaders to learn from different perspectives

and experiences, understand how these challenges are emerging across society and public life, and respond to them in informed and effective ways.

As our work develops, I would be very happy to share those insights, and the lessons from our wider transatlantic collaboration, with this Committee.

Thank you and I welcome your questions.