

Kate Jones, CEO, Digital Regulation Cooperation Forum

Keynote speech at IAPP Data Protection Intensive London – 13 March 2025

The AI transition: is your governance ready?

When my children were smaller, I used to enjoy taking them to a living history museum that let them experience life in Victorian and 20th century Britain. Aside from the excitement of gas masks and air raid shelters, their favourite part was always being issued with a ration card and taking it along to the old-fashioned sweet shop. But for grown-ups like me, the museum's impressive exhibition of steam engines was fascinating: it brought to life how these devices must have seemed so huge, noisy, complex and frankly overwhelming even as they made such transformative changes, not only to transportation but also in heralding the industrial revolution.

AI is to this second quarter of this 21st century as the steam engine was to Victorian Britain: it is catalysing developments that will reshape our world. Unless perhaps you work in a data centre, AI is not large and noisy like the early steam engines – but it's certainly complex and overwhelming. 2025 is a pivotal moment: if I were a historian in the future, 2025 is the year of digital and AI governance that I would want to study.

Why 2025? Because it is the inflection point: now is the time our world is changing. If you listen to the current US conversation, you will hear that some GenAI developers are anticipating that artificial general intelligence, AGI, will be with us as early as 2026. In very general terms, we're talking about AI that can do most things that humans can currently do while sitting at a computer. I don't think anyone fully understands yet what the consequences will be, but they may well be seismic: the world in 2030 could look very different from today. The governance architecture we erect right now, in 2025, may have lasting impact - not only in 2030 but on generations to come.

As a digital regulator, my focus is firmly on that governance architecture. And my key question for you all, as the privacy community, is this: how are you using the brilliant skills and expertise you have today, to prepare and implement frameworks ready for this transition? Or to put it another way – when you visit the living history museum of the future, what will each of you say was your contribution to governance, at the inflection point of 2025?

Governance goal

In a moment I am keen to highlight three changes in the governance world that have been or ought to be coming to you as privacy professionals; but let me first propose an overall goal for you all that derives from two propositions.

First, that privacy has never been more important. The prospects of what could be done to any of us by ignoring our privacy are terrifying, and some of them we are already seeing: from acts that are criminal such as fraud and extortion, to the ‘merely’ exploitative such as manipulating how we think and what we believe, to the commercialisation of the most intimate aspects of ourselves, our human needs and our values. I saw in the press last week a journalist’s investigation revealing that right now, a large US company is offering advertisers segmentation of its users by such sensitive data points as people in chronic pain, and people who are in financial distress; not to mention those who are judges, or military, or Capitol Hill workers. You are on the front line of protecting people and your work is incredibly important.

Second, that on the other hand, we live in a world where Governments, including here in the UK, are looking to data, technology and AI to drive innovation and growth. It’s data that is enabling breakthroughs in medicine, improving safety in infrastructure, and generating efficiency in the workplace. Data is our future. As the governance community, our role is not to try to prevent the harnessing of data, and not to be a brake on innovation, but to ensure that it’s done in responsible ways.

Our goal overall, therefore, must be to make these two propositions compatible: we need to enable data use and innovation while also protecting privacy.

Three changes

With that goal in mind, I turn to three developments in governance that I see as essential. These are a new focus on data; the ending of siloed governance; and harnessing regulation to embrace innovation.

FIRST, we are living through a transition to a data-based economy. It may not be an exaggeration to describe some of our largest businesses – from banks to supermarkets - as data management companies with respectively financial services or retail functions attached. As a result, my expectation is that many of you with responsibility for privacy now also have a strategic

responsibility for managing your organisation's data. And indeed, this responsibility is becoming essential, alongside protection of privacy.

The question here – and it's not a new question, but it's one that really does need resolution at this 2025 inflection point - is: How can we give more meaningful control to individuals over their own data at the micro level, while still enabling data sharing at the macro level? Let's say a person – such as you, or me - would like to give permission for her data to be used for some purposes, such as medical research, or anonymous training of models, while saying 'no thanks' to other purposes, such as targeted ads – and doesn't want to have to keep repeating that message? I am confident there is much more to be done in this space, particularly as we see the arrival and embedding of digital verification services. Your challenge, as the privacy community, is to think creatively about how we can enable business use of data while protecting individual people's privacy in ways that are meaningful and aren't intrusive.

The SECOND development – and it won't surprise you to hear this from me - is the ending of siloed governance. New technologies often engage multiple regulatory remits at the same time. Look at AI governance: it engages privacy and data protection, equality and human rights, online safety, consumer protection, competition – not to mention sectoral regulation such as in financial services, medicine or other areas.

And it does so in ways that closely intersect. Let's take online safety and privacy. Ofcom is deeply immersed in implementing the Online Safety Act to secure children's safety online. You will have seen their draft Children's Safety Codes and age assurance guidance. At the same time, the ICO is equally deeply concerned with how digital platforms are using children's personal information and has recently announced investigations into how TikTok and others are using it. Through my organisation the DRCF, those regulators can ensure coherence in their activities. I could give plenty of other examples, and as we see technologies come together more in future – for example AI and robotics, or AI and quantum – these intersections will only increase.

You can't navigate all that without joining up. The regulators ended their silos some time ago. The DRCF, which I have the honour to lead, was established to bring together the key UK digital regulators. Over the last 5 years we've become closer in addressing shared challenges, while respecting each regulator's independence. Our work together has ranged from setting up a multi-agency advice service, through research and reporting on regulatory implications of emerging

technologies such as quantum, digital ID and soon on agentic AI, through to ensuring coherence in our policy guidance and supervisory functions.

Just this week, the CEOs of the FCA and the ICO issued a joint letter through the DRCF, inviting industry leaders to a joint roundtable on 9 May to discuss how their organisations can work together with industry to support growth and promote regulatory certainty as AI is deployed in financial services.

At the DRCF we have a unique perspective: we have a lens on to the impact of multiple regulatory remits on the digital and AI landscape. Harnessing that birdseye perspective, I see you, the privacy community, as vital to the responsible implementation of AI. I have a specific call for you.

The AI governance picture sometimes looks messy: there are lots of building blocks. You – privacy experts – should be the mortar that holds all those bricks together, creating a smooth, weight-bearing wall of shared responsibility for digital and AI governance; one that’s strong enough for your Board to rely on. Why you? For two reasons.

One, because in our experience at the DRCF, data protection is the most common single theme of digital governance. When we reviewed all the DRCF’s projects recently, we found that more of them involve ICO than any other regulator.

Two, because you have expertise in risk management, in preparing cross-organisation impact assessments and mitigating risks efficiently. My call, therefore, is for you to thread your expertise well beyond the data protection field, because you can help your organisation navigate all its digital governance requirements at once.

That brings me on to the THIRD development in governance, the innovation space. This is the exciting part. Enabling innovation is critical for economic growth, and an integral part of the vision of the DRCF. The biggest challenge of this 2025 AI inflection point is how we establish and implement parameters that enable innovation while avoiding harms, thereby engendering public trust and confidence. Regulators are implementing tools to enable speedy adoption and scaling of innovations – take for example the DRCF AI and Digital Hub, which has enabled digital innovators to seek free and informal advice from all our regulators at the same time. As we work, as regulators, to become more agile, we are looking for a more evaluative approach from you in industry too.

Indeed, the step change of recent years, as I am sure you know, is a move towards risk-based, outcome-focused regulation. Let me take the FCA's consumer duty as an example: it puts the onus on financial services firms to support the delivery of good outcomes for customers. As a result, it's creating a foundation of customer trust in the UK financial services industry on which firms can build innovation and tech development safely and on a level playing field without a constant need for new rules.

I know this shift towards outcome-based regulation is challenging for industry, not just for compliance teams but in the C suite. But look at this as an opportunity for the privacy community: to bring you a new energy as strategy enablers. You have valuable experience of risk-based regulation. You can promote innovative approaches which enable your business to meet ongoing requirements of privacy and safety by design, while reassuring your colleagues that you have the tools your business needs to assess and mitigate risks on an ongoing basis. You should be closer to Board-level decision-making than ever before, finding ways to enable innovation and mitigate risks. In my view, this is the significant contribution you can make at this AI inflection point of 2025.

To conclude, in case I haven't been clear, the race for digital and AI innovation certainly doesn't mean abandoning responsibility. Protecting people is a key element of the DRCF's vision, alongside empowering innovation. But we should be harnessing current strengths – including your strengths as privacy professionals – to enable innovation while mitigating risks. Good regulation, implemented to facilitate responsible innovation rather than to obstruct it, facilitates economic growth.

I wonder what the technology section of the living history museum of the 21st century will look like: what shifts the AI transition is going to bring us in practice. Hopefully, it will be more meaningful than holographic social feeds and crazy robots, even if those are the fun part for tomorrow's children. In the small print for grown-ups, I wager the museum will say that 2025 was the year when AI governance matured. Through responsible data management that respects privacy; through collaborative working across sectors; and through a risk-based approach to enabling responsible innovation: let us all shape effective governance that is ready for the AI transition.