Emerging approaches to the regulation and enforcement of AI use (a UK perspective)

Gareth Oldale, Partner and Head of Data, Privacy and Cybersecurity, and Emily Holdsworth, Legal Director, TLT LLP, compare the approaches from some of the key AI regulators in the UK

Prior to the dissolution of UK Parliament at the end of May 2024, the Science, Innovation and Technology Committee of the House of Commons published its third report on the governance of AI ('the Report'), examining domestic and international developments over the last year. A key theme of the inquiry was whether the government should bring forward AI-specific legislation. Resolving the scope of such legislation will no doubt be a priority for the next government.

The Report concludes that the success of the UK's current pro-innovation approach will be determined to a significant extent by the ability of sectoral regulators to put the five high-level principles outlined in the government's AI White Paper into practice. Three factors will influence their ability to deliver: powers, coordination and resourcing.

The next government will need to continue to prioritise a regulatory gap analysis to determine whether regulators require new powers to respond to the growing use of AI. It will also need to address the need for coordination between regulators where their remits overlap. On resourcing, the Report considers that the sum of £10 million allocated by the previous government is clearly insufficient for regulators to meet the new challenges.

Sectoral and cross-economy regulators in the UK were asked to publish an update by the end of April on how they are taking forward the White Paper proposals and the steps they are taking to develop their strategic approaches to AI. These have now been published by the Department for Science, Innovation and Technology.

In this article, we compare the approaches from some of the key regulators, namely the Information Commissioner's Office ('ICO'), the Competition and Markets Authority ('CMA'), the Financial Conduct Authority ('FCA'), the Office of Communications ('Ofcom') and the Office of Gas and Electricity Markets ('Ofgem'). It is clear that AI is a topic very much at the top of their agendas.

ICO

The ICO's strategic approach welcomes the government's approach to build on the strengths of its existing regulators, who it considers are well-placed to tackle the AI risks that emerge in their context. Wherever processing of personal data takes place in the development and deployment of AI systems, this will fall under the ICO's purview. The ICO therefore has the ability to intervene right across the AI supply chain, and it considers that data protection law can mitigate many AI risks.

Being principles-based, data protection law provides a flexible framework that enables organisations to adapt to evolutions in AI technology. The ICO notes that the principles set out in the White Paper (namely: safety, security and robustness; appropriate transparency and explainability; fairness; accountability and governance; and contestability and redress) closely mirror the statutory principles the ICO already oversees. It points to guidance it has already produced, such as security and data minimisation in AI, explaining decisions made with AI, how to ensure fairness in AI and the accountability and governance implications of AI. While the contestability and redress principle is not a principle of data protection law as such, it is instead reflected in a set of information rights that individuals can exercise, such as the right of access.

The ICO points out that AI is not new; it has already been regulating this field for over a decade, producing a range of guidance products, tracking developments to detect new data protection risks, and assisting with the development of new products via its Regulatory Sandbox. It launched a consultation series on generative AI in January 2024 (for the latest update, see Volume 24, Issue 8, page 1), and a further consultation is planned on biometric classification technologies.

As a whole-economy regulator, the ICO works closely with a wide range of other regulators and is a founding member Digital Regulation Cooperation Forum ('DRCF') through which it works with the CMA, Ofcom and the

FCA to deliver a coherent approach to digital regulation.

CMA

In its AI strategic update, the CMA states that it, too, has been considering the impact of AI on competition and consumer protection issues for a number of years. It has published papers on the risks posed by algorithms and also on AI foundation models ('FMs'), including a technical update report in April which highlights the complex foundation model value chain that AI-powered services are built upon. The CMA's strongest competition concerns arise from the fact that a small number of the largest incumbent technology firms could profoundly shape the development of AI-related markets to the detriment of fair, open and effective competition. It also considers that AI has significant scope to facilitate unfair consumer practices.

The CMA has recently updated its set of six principles to guide the ongoing development and use of FMs. These principles are intended to complement the government's approach and its cross-sectoral AI principles but, in view of the CMA's remit, are focused on the development of well-functioning economic markets that work well from a competition and consumer protection perspective. These are as follows:

- Access — ongoing ready access to inputs to enable ability to compete;
- Diversity — sustained diversity of business models and model types, including both open- and closed-source;
- Choice — sufficient choice for businesses and consumers so that they can decide how to use FMs;
- Fair dealing — no anti-competitive conduct such as self-preferencing, tying or bundling;
- Transparency — consumers and businesses have the right information about the risks and limitations of FMs so they can make informed choices; and
- Accountability — FM developers and deployers are accountable for FM outputs.

"Whichever party is elected, and whatever plans for AI legislation emerge over the next few months, it will remain important for regulators to continue to develop detailed guidance for their sectors and to continue to prioritise their work in identifying emerging risks."

Acknowledging the importance of collaboration with other regulators, the CMA points to the joint research it is undertaking (as part of the DCRF) into consumer use and trust of generative AI, and developing its understanding of algorithmic processing, AI auding and AI governance. It is clear that the CMA will be scrutinising developments in FM-related markets closely when deciding which digital activities to prioritise for investigation under its new powers granted by the Digital Markets, Competition and Consumers Act.

FCA

As stated in its AI update, the FCA is a "technology-agnostic, principles-based and outcomes-focused regulator" and therefore welcomes the government's approach. The FCA's focus is on how firms can safely and responsibly adopt AI technology, as well as understanding what impact AI innovations are having on consumers and markets.

The FCA already has a number of frameworks in place which are relevant to firms' safe use of AI, including the FCA's Principles for Business and other rules and guidance, such as the Consumer Duty and the Senior Management Arrangements, Systems and Controls ('SYSC') sourcebook. The update outlines how some of the key elements of these frameworks map to each of the government's five principles.

The FCA will continue to collaborate closely with the Bank of England, the Payment Services Regulator and with other regulators through its membership of the DRCF, as well as prioritising international engagement on AI. Its action plan for the next 12 months includes continuing to further understand AI deployments in UK financial markets and actively considering whether future regulatory adaptations are needed. It is keen to emphasise that it actively supports testing for beneficial AI, through its Regulatory Sandbox and Digital Sandbox, TechSprints and other innovation advisory services.

Ofcom

Ofcom published its update on its strategic approach to AI 2024/25 on the same day as its plan of work for 2024/25. It considers that the government's AI principles are "a useful lens" through which to consider its work on AI and are broadly aligned with the underlying principles of its regulatory regimes.

Ofcom refers to the Online Safety Act as an example of where similar principles have been actively considered by Parliament and underpin Ofcom's legislative framework. Both the AI principles and Ofcom's key outcomes for online safety emphasise the importance of appropriate accountability and governance, safety and transparency. With regard to fairness, Ofcom wants users to have the choice to control the content they see and have contestability and redress options if they want to report harmful content.

In addition to its powers under the Online Safety Act, Ofcom points to the 'general conditions' for telecoms

(Continued on page 6)

(Continued from page 5)

providers as part of its duties under the Communications Act 2003. AI can enhance the sophistication of scam calls, and Ofcom has the power to instruct providers to block access to numbers or services on the basis of fraud or misuse. Under the Telecommunications (Security) Act 2021, Ofcom has a duty to ensure that telecoms providers take appropriate and proportionate measures to identify, reduce and prepare for security risks. Providers can use AI to monitor for abnormal activities and identify potential vulnerabilities. Ofcom also holds competition and consumer powers concurrently with the CMA which could apply to digital services.

Ofcom has a wide programme of work to identify AI risks and opportunities, but it selects three areas to highlight the cross-cutting risks and its work to address them. The first is synthetic media, where AI can be used to create harmful content, misinformation and personalised scams. The second is personalisation of content to users, and the third is security and resilience, in particular the risk that more advanced forms of AI could be used to develop more virulent malware or provide instructions on how to breach network security. As some companies regulated under the Online Services Act are at the forefront of AI developments, Ofcom has also carried out additional work in this area and will continue to do so, along with other regulators via the DRCF. It also highlights its work with other regulators across the globe.

Ofgem

Ofgem's strategic approach to AI is brief in comparison, but more detail is set out in its earlier call for input in April, which sets out how it will address specific risks relating to AI and its impact on the consumer, market, company and sustainability. An understanding of the potential risks will allow Ofgem to develop guidance and tools that make sure that:

- use of AI is fair, ethical, transparent and explainable. AI has the potential to improve service to consumers, but also has the potential to exclude certain customers causing discrimination and inequality;
- use of AI results in fair market outcomes. Ofgem is working with the CMA on potential solutions to address concerns on the use of algorithms which make it easier for companies to engage in 'tacit collusion';
- energy companies have effective oversight of AI systems. Governance measures should be in place to ensure effective oversight of the supply and use of AI systems, with clear lines of accountability across the AI life cycle. A multi-regulatory approach will be required to join up regulation;
- customers have appropriate redress routes to contest negative outcomes; and
- use of AI is on a sustainable basis. AI is already being utilised to support sustainability through identifying and signalling problems and detecting equipment failures, but AI models consume substantial amounts of energy and water. Ofgem's AI taskforce is exploring these issues further to ensure that the UK's Net Zero carbon emission objectives are not undermined.

What next?

The pace of legislative and regulatory change regarding the use of AI has been rapid over the last year, with moves by both the United States and European Union to develop their own approaches to AI governance.

At the time of writing, the outcome of the General Election on July 4th is not known. Whichever party is elected, and whatever plans for AI legislation emerge over the next few months, it will remain important for regulators to continue to develop detailed guidance for their sectors and to continue to prioritise their work in identifying emerging risks.

As the Report states, sectoral guidance should help deployers "strike the balance between the protection of privacy and securing the technology's intended benefits. In instances where regulators determine that this balance has not been met, or where the relevant laws or regulatory requirements have not been met, it should impose sanctions or prohibit the use of AI models or tools."

Gareth Oldale and Emily Holdsworth
TLT LLP
gareth.oldale@TLTsolicitors.com
emily.holdsworth@TLT.com