LOOKING BACK AT 2022:

TECHNOLOGY & DIGITAL, INCLUDING CYBER SECURITY

WELCOME

Almost 12 months ago and shortly after welcoming in the New Year, Sally Mewies and Luke Jackson from our Technology & Digital Group gave their predictions for what to look out for in 2022, highlighting ten legal and regulatory developments we expected to see this year including in relation to cyber security, data reform, AI regulation and more. Now, as we approach the end of the year, we take the opportunity to reflect on what came to pass (and what didn't) in 2022. We'll be looking forward to 2023 in our next publication.

We publish a regular round-up of legal and non-legal tech-related news stories (see our latest edition here): to receive this and other similar updates direct to your inbox, click here to register.

LOOKING BACK

Data protection and e-privacy reform

Fast forward a year and we're still waiting for concrete proposals on post-Brexit data protection and e-privacy reform. The Data Protection and Digital Information Bill presented in July was put on hold in September as Prime Ministers came and went. We're waiting to hear more about the "business and consumer-friendly, British data protection system" announced in October by the new Secretary of State. As is the EU, which is keeping a close eye on reforms and their potential impact on data adequacy.

The ICO's international data transfer agreement and UK addendum to the new EU standard contractual clauses came into force in March. They replaced use of the old EU SCCs for transferring personal data outside of the UK in the absence of relevant adequacy arrangements. And just in the past few weeks the ICO published updated guidance on international transfers, with more to come. We've also seen movement on possible UK/US and EU/US data transfer frameworks.

The ICO's revised approach to public sector enforcement resulted in the Department for Education avoiding being issued with a £10 million fine. And the new Information Commissioner recently said that fines are still an important enforcement tool that will be used where they are truly needed, but stressed they are only one of a number of tools available.

Increased scrutiny of 'Big Tech'

The Big Tech companies have rarely been out of the news this year; as governments, regulators and consumers around the world seek to crack down on online harm and alleged anti-competitive and other practices.

The Online Safety Bill now looks to be moving forward after suffering delays following the changes in government. The new UK competition law regime for the most powerful digital firms, overseen by the Digital Markets Unit, was expected to be introduced in 2022. It's now likely to happen in 2023, after the Chancellor confirmed in the Autumn Statement that the government will bring forward the Digital Markets, Competition and Consumer Bill. In other developments, the FCA launched a discussion on the competition impacts of Big Tech on the financial services industry.

Meanwhile, over in Europe, the Digital Markets Act and the Digital Services Act came into force. Together they form the digital services package, the EU's response to the need to regulate the digital space.

The digital supply chain

Effective supply chain management has been a key focus for businesses as they continue to experience disruption from Brexit, the pandemic, and now the war in Ukraine. Under pressure from rising costs and labour and materials shortages, businesses across a wide range of sectors have turned to digitalisation to reduce costs, increase efficiencies, aid transparency and, crucially, improve sustainability. This insight on our Factory of the Future microsite gives a flavour of the different innovations being deployed.

We've seen initiatives such as the Made smarter innovation challenge and the Smart Manufacturing Data Hub. An Electronic Trade Documents Bill was introduced to make digital documentation legally recognised, reduce admin costs and make it easier for British firms to buy and sell internationally. Microsoft joined other tech companies in offering sustainability tracking products as companies have increasingly focused on the ESG agenda; and the National Cyber Security Centre issued guidance following a rise in supply chain cyber attacks.

Regulation of AI

The government published a new AI paper, outlining its approach to regulating the technology in the UK and calling for views until 26 September. The government's long-awaited AI White Paper and public consultation was expected in the first half of 2022, then in late 2022. We're still waiting for it.

In other UK developments: the three financial regulators published a joint discussion paper on AI in financial services; the House of Commons Science and Technology Committee launched an inquiry into AI governance; the government published the response to its consultation on how AI should be dealt with in patent and copyright systems; the ICO launched its AI toolkit; the Medicines & Healthcare products Regulatory Agency took steps towards regulation of software and AI as a medical device; and the Transport Committee is currently examining emerging regulation for self-driving vehicles.

There's also been a flurry of activity over in Europe; including a proposal for an AI Liability Directive aimed at making it easier for victims of AI-related damage to get compensation. Our recent briefing outlines other proposed reforms touching on AI regulation.

Financial services

It's fair to say many of the discussions around tech and financial services this year have focused on cryptoassets, the high-profile collapse of the FTX cryptocurrency exchange providing the most recent example. This development was discussed as the Treasury Committee held its first evidence session in its inquiry into the cryptoasset industry. At the moment, cryptoasset regulation is limited to registering of UK-based cryptoasset exchanges for anti-money laundering purposes. The Crypto and Digital Assets All Party Parliamentary Group announced details of its own wide-ranging inquiry into the UK's crypto and digital assets sector; the FCA held various CryptoSprints, exploring how cryptoassets could be regulated in the UK; plans are underway to bring cryptoassets within scope of financial promotions legislation; and the Financial Stability Board published a proposed framework on the international regulation of cryptoasset activities.

Throughout the year the courts consistently showcased England and Wales as a leading jurisdiction for dealing with actions involving cryptocurrencies and other digital assets.

Various countries are making moves towards introducing central bank digital currencies. The Bank of England says it's looking carefully at how such a currency might work, but it hasn't yet made the decision to introduce one.

In other developments, the FCA: held an Innovation Open Day in July; ran an authorised push payment fraud TechSprint in September; and launched a Diversity, Equity and Inclusion Spotlight initiative, saying that FinTech has an important role to play in driving financial inclusion.

Increased emphasis on cyber security...

The National Cyber Security Centre's recently published Annual Review says that ransomware remains the most acute threat that businesses and organisations in the UK face. The cyber threat also evolved significantly this year with the war in Ukraine. We've seen various guidance issued throughout the year, including joint advisories with the NCSC's international partners on supply chain security and the increased globalised threat of ransomware. The Joint Committee on the National Security Strategy launched an inquiry into ransomware at the end of October.

The government published the 2022 cyber security incentives and regulation review, following on from the release of its National Cyber Strategy 2022 at the end of 2021. It revealed that UK organisations don't currently have enough robust measures to successfully defend against the rapidly increasing risk of cyber attacks. Consultations were published on: proposed legislation to improve the cyber resilience of organisations important to the UK economy; and embedding standards and pathways across the cyber profession by 2025. There was also a call for views on how to boost the security and resilience of the UK's data centres and online cloud platforms.

Over in Europe, the European Parliament adopted new legislation setting tighter cybersecurity obligations for: risk management; reporting obligations; and information sharing.

...that will also impact consumers

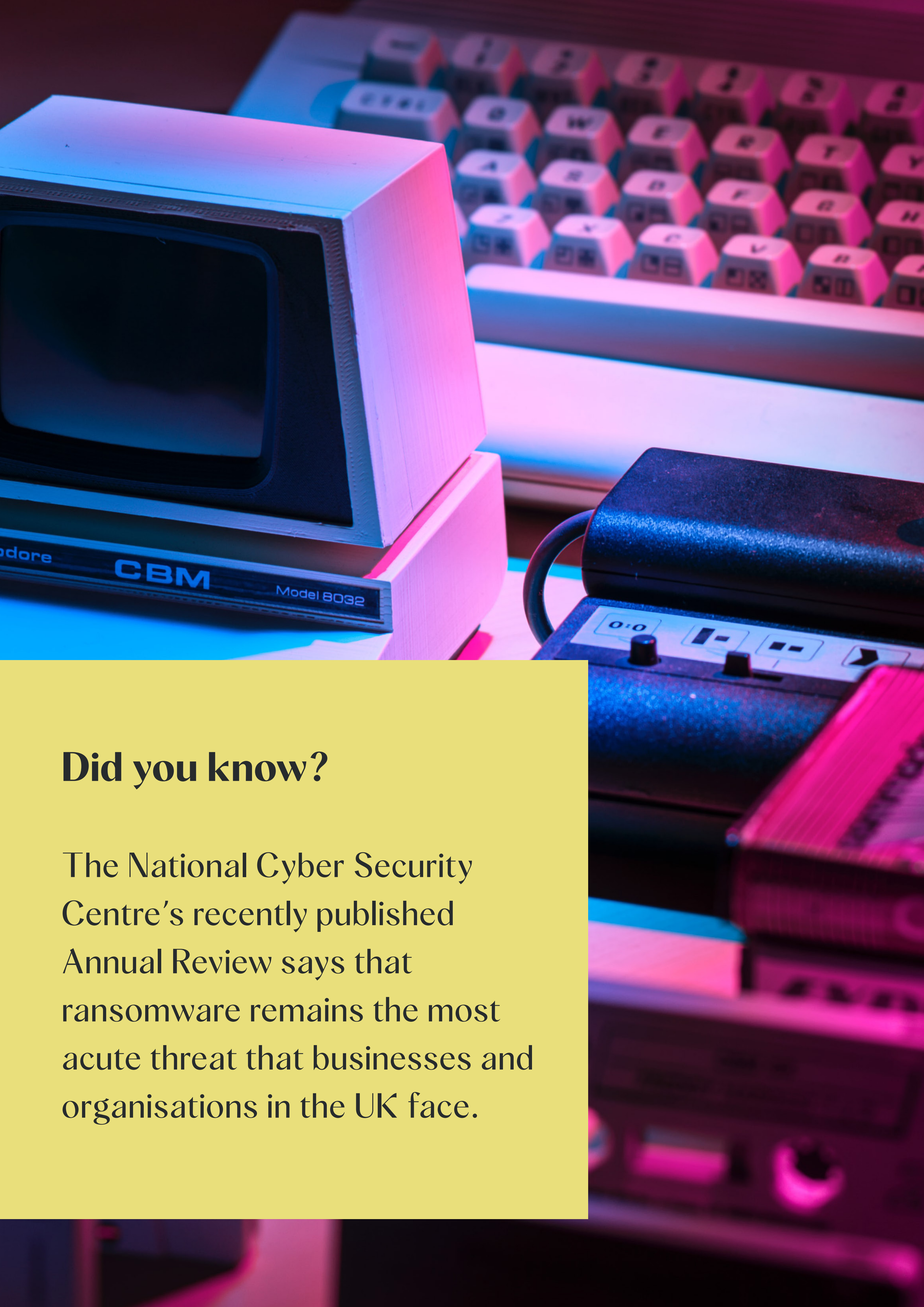
The Product Security and Telecommunications Infrastructure Bill is due to become law by the end of the year. This House of Commons Library Research Briefing explains the main provisions. Details of the security requirements that manufacturers, importers and distributors of consumer connectable products will have to comply with will be published in separate regulations. We expect a transition period prior to implementation. Similar to GDPR, the maximum fine for non-compliance is £10 million or 4% of qualifying worldwide revenue. The NCSC's CEO outlined in a recent speech how the 'secure by design' approach encapsulated in the Bill is vital for managing Internet of Things risks.

In related developments: the UK, Canada and Singapore agreed to work together to promote and support cyber security measures for internet connected products; the Digital, Culture, Media and Sport Committee launched its 'Connected tech: smart or sinister?' inquiry to examine the impacts of the increasing prevalence of smart and connected technology and what needs to be done to make sure it's safe and secure for its users; the NCSC launched a package of support to help retailers protect themselves and their customers online; and the government consulted on plans to improve the security and privacy of apps and app stores.

Over in Europe, the Commission proposed a Cyber Resilience Act to protect consumers and businesses from products with inadequate security features.

Increased collaboration

We've seen so many examples this year of collaboration between governments, regulators and other bodies, both nationally and globally; in particular in relation to cryptoasset regulation, data protection and cyber security. Our world is so inter-connected, it's recognised that significant global cooperation is needed to guide national regulation and supervision. On the other hand, in a report on digital trade, TheCityUK warned that the world risks fragmenting into regional and national 'splinternets' unless governments can agree on a shared approach to data regulation and cross-border data transfers.



Did you know?

The National Cyber Security Centre's recently published Annual Review says that ransomware remains the most acute threat that businesses and organisations in the UK face.

This is particularly important post-Brexit, and not just in relation to data.

Smart contracts and blockchain

In July we produced a round-up on blockchain, NFTs and smart contracts - taking a look back at the highlights from the first half of the year and considering what we might expect to see in the future.

There's been a flurry of activity in this area. LawtechUK and its UK Jurisdiction Taskforce launched the 'Smarter Contracts' project to encourage increased understanding of smart contracts and blockchain technology and how they are being used. The Taskforce also recently consulted on how English law can support the issue and transfer of equity or debt securities on blockchain and distributed ledger technology systems.

The Law Commission's been particularly busy too. We've seen: a consultation on provisional law reform proposals to make sure the law recognises and protects digital assets; the launch of a review of how private international law applies to digital assets and other emerging technology; and a recent call for evidence on how decentralised autonomous organisations can (and should) be characterised, and how the law of England and Wales might accommodate them now and in the future.

Our commercial dispute resolution experts considered Law Society guidance on blockchain technology and its impact on the dispute resolution process and offered their insights into the court's significant decision to allow service of documents via the blockchain.

Click here for our webinar recording 'Blockchain and Sustainability – Friends or Foes?' where we looked to dispel some of the myths surrounding blockchain and discussed topical issues such as energy efficiency and sustainability.

Web3, NFTs and the metaverse

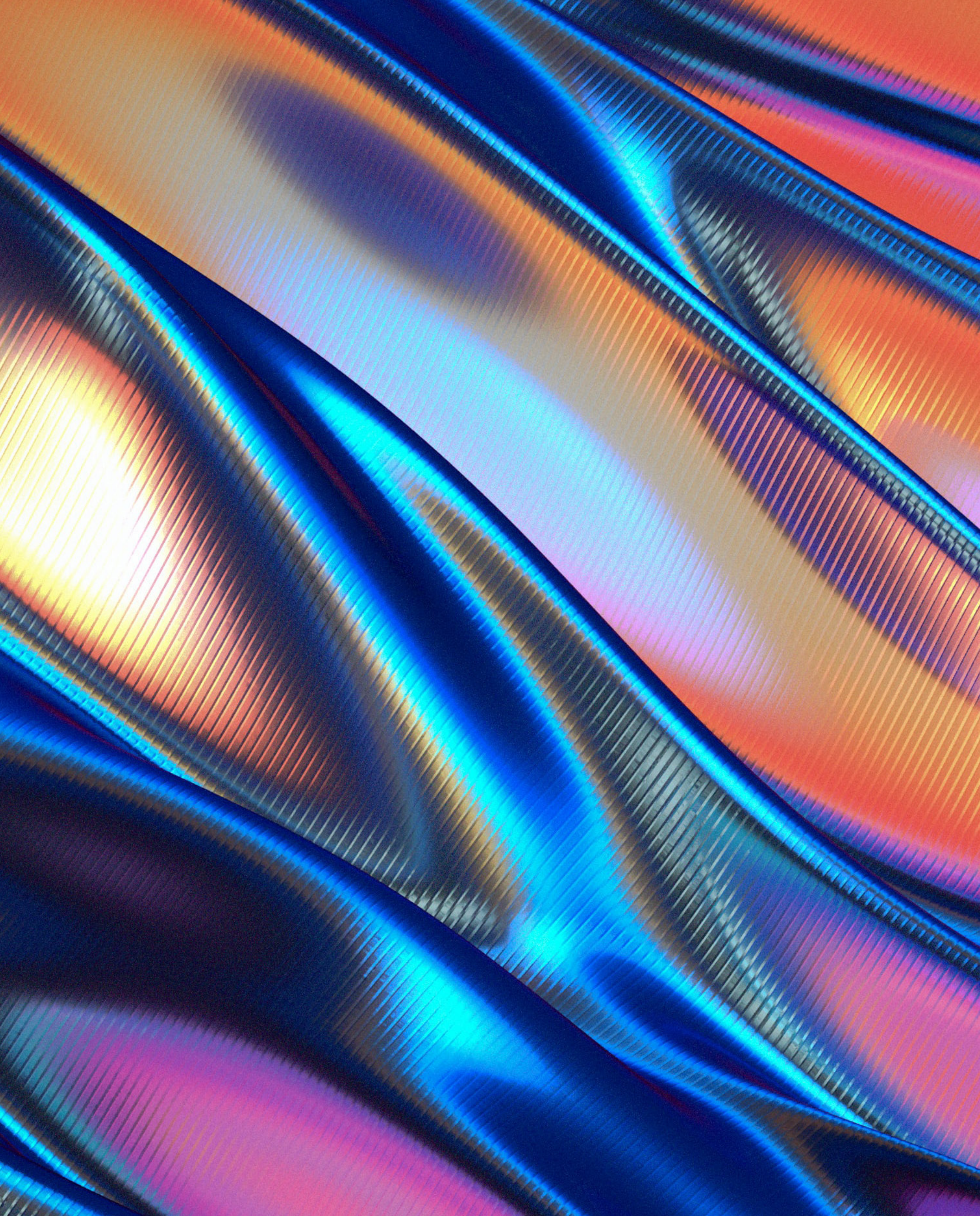
We've already touched on the discussions around crypto regulation and the Law Commission's various projects on emerging technologies. In November, the Digital, Culture, Media and Sport Committee launched an inquiry into the operation, risks, and benefits of NFTs and the wider blockchain. The inquiry is likely to examine whether more regulation is needed, ahead of a Treasury review.

Despite a sense that the excitement might be waning, we've seen numerous examples in 2022 of businesses launching digital collections, entering the NFT marketplace and setting up shop in the metaverse; from retailers and publishers to banks and sports clubs. And when Meta boss Mark Zuckerberg recently announced the loss of 11,000 jobs, it was made clear that the company's long-term vision for the metaverse is one of its high-priority growth areas. Watch this space.

CONTACTS

SALLY MEWIES
Partner
Head of Technology & Digital
+44 (0)771 083 6704
sally.mewies@walkermorris.co.uk

LUKE JACKSON
Director
Technology & Digital
+44 (0)781 693 3684
luke.jackson@walkermorris.co.uk



www.walkermorris.co.uk
T +44 (0)113 283 2500
F +44 (0)113 245 9412

Walker Morris LLP
33 Wellington Street
Leeds
LS1 4DL