CLIFFORD
CHANCE

TECH TRENDS 2023

— THOUGHT LEADERSHIP

FEBRUARY 2023

TECH TRENDS 2023

Evolving technologies, increased digital connectivity, cyber risk, geopolitical tensions, climate change, supply chain disruption and changing markets are shaping government policies, regulation and legal risk in relation to the use of data and technology. This legal, economic and political landscape is informing board agendas and investment approaches as businesses review and refocus their digital strategies. We look at the data and technology trends to watch in 2023.

Part1 – Digital Regulation and Strategy

1

Cyber gets serious

As reliance on digital infrastructure increases and data becomes more voluminous, valuable and vulnerable, we expect to see a rise in cyber incidents and attacks. "Cyber wars" between nations are predicted to be major threats to critical national infrastructure and services, as well as targeted ransomware attacks. With a flurry of new and revamped legislation impacting cybersecurity and operational resilience, regulatory requirements are becoming more numerous and stringent, often with formidable associated enforcement regimes.

What's next?

- **More sophisticated attacks:** Deployment of artificial intelligence (AI) and machine learning technologies will become an increasingly critical component of the arms race between company security teams and cyberattack perpetrators. This increased automation of the security and attack process could see organisations fending off countless hyper-speed attacks each day. The next generation of cyberattacks will move from opportunistic to targeted, and deepfakes and natural language chat bots could move phishing attacks to the next level.
- **Incident management navigation:** The management of cyber incidents will become increasingly complex as more laws come into force, existing laws are revised, and the trend of multiple regulators investigating cyber incidents continues. Increasingly, companies are subject to legal requirements to have incident response plans. Even where not legally required, companies are relying on such plans to navigate the various incident management and reporting requirements under a patchwork of laws governing cybersecurity and resilience, ransomware payments, privacy and, often, sector-specific requirements and regulators.
- **Supply chain risk:** Management of cyber and operational resilience risk in the extended supply chain will be crucial across sectors. Supplier due diligence, audit and robust contractual terms will be key tools in managing risk exposure and securing crucial rights and recourse in the event of an incident or failure of a supplier. In certain sectors, this risk management will be required by law. Beyond these sectors, supply chain risk management will be in the spotlight due to increasing client requirements and growing risk awareness. This will impact supplier engagement as well as due diligence for M&A activity.
- **Connected devices:** With the EU's proposed Cyber Resilience Act seeking to raise the cybersecurity standards for connected hardware and software placed on the EU market, in 2023 we will see manufacturers, importers and distributors of a vast range of digital products and applications engaging with, and preparing for, this regulation as it makes its way through the EU legislative process and is expected to influence manufacturing, import and distribution standards globally.

For more, see our briefings: NIS 2 Directive: Europe revamps its cybersecurity framework; EU Cyber Resilience Act - Proposed Cyber-Security Rules for Connected Products; and DORA: What the new European framework for digital operational resilience means for your business.

Data in the spotlight

2

The proliferation of heavy-hitting data protection laws continued in 2022. We are seeing some laws come into full effect as well as regimes developing the specificity of their requirements and others strengthening their sanctions. Privacy enforcement has been active, including large GDPR fines and the first ever CCPA enforcement action. Joining the data governance landscape are new laws and proposals tackling how certain data sets – containing both personal and non-personal data – may be shared and used.

What's next?

- **Increased complexity in data governance and transfer:** Significant new privacy laws and changes to data protection regimes are on the horizon in 2023 – including in the USA, the UK, India, Nigeria and Saudi Arabia. Alongside these privacy developments, we will also see wider data governance laws and frameworks being introduced or developed, with the European Union (EU) leading the charge as the Data Act and the Common European Data Spaces initiative follow hot on the heels of last year's enactment of the EU's Data Governance Act. The increase in the number of such laws – some with extraterritorial effect, and with application to increasingly broad types of data – means that multinational organisations face increasingly complex data governance and risk management. In 2023, many businesses will be reviewing their data infrastructure, policies, processes, supplier engagements and risk positions to tackle data governance requirements and data transfer frictions in a pre-emptive and holistic manner, as well exploring the use of new technologies such as privacy-enhancing technologies.
- **International co-operation for data transfers:** High-profile enforcement activity in relation to data transfers has put pressure on international co-operation efforts to facilitate legal transfer of data between continents. With momentum building behind the Global Cross-Border Privacy Rules Forum and progress of the EU-US Data Privacy Framework expected to be fast-paced, we should see businesses being able to meaningfully leverage related transfer mechanisms. Of course, the testing of these frameworks in court will doubtless follow.
- **Enforcement and litigation risk:** Data governance will remain a key area of legal, operational and reputational risk across sectors in 2023, given the severe and active regulatory enforcement regimes and increasing cost and risk of litigation. We will see forms of group redress or class actions centring on privacy issues in many jurisdictions. Key areas of focus for regulators and courts this year are expected to be the processing of children's data and biometric data, automated decisions, data monetisation and transfers. There will also be sustained attention on the intersection between privacy and antitrust as the use of data by big tech companies is scrutinised.

For more, see our articles: Next steps after U.S. President Biden issues Executive Order on U.S. data transfers from 'qualified state and Beyond adequacy: working together to ease multi-jurisdictional privacy compliance.

The AI legal landscape evolves

3

We are seeing significant evolutions in the capabilities of AI and machine learning technologies – including generative AI with greater capacity for seemingly creative action and personalisation. Interactions with other emerging technologies, such as neurotechnology and quantum computing, could hugely accelerate these developments. This presents both exciting opportunities and a range of legal, ethical and practical questions. In 2023, we will see significant milestones in the development of the regulatory frameworks for AI, and businesses will be stepping up their internal capabilities to develop, deploy and manage AI in a legally compliant and ethical manner.

What's next?

- **Evolving legal frameworks:** The EU's AI Regulation is expected to be finalised and adopted in the year ahead. It will sit alongside the proposed AI Liability Directive in regulating how AI can be used and who is liable for harms caused by use of AI. The UK is expected to issue an AI framework to underpin sector-specific rules. In the US, we expect to see progress of the AI Bill of Rights, and the testing of the practical

application of New York City's law governing AI in recruitment. China's regulatory architecture for AI is expected to continue to emerge following its regulation on recommendation algorithms coming into effect last year and its recently released measures on production of 'deepfakes'. Such AI-focused legislation will form part of the landscape of privacy, product safety, consumer protection and other laws which regulate the use of AI.

- **Ethics and risk management:** Businesses will also be navigating ethical and risk management frameworks that will influence market practice, shape customer expectations and inform regulatory views of appropriate AI development, deployment and governance. Standards organisations and hubs are expected to release AI-related standards and guidance. In turn, we will likely see the rise of AI assurance ecosystems and audit services, as well as businesses making greater investments in hiring, developing and retaining talent that can deliver AI projects responsibly and oversee the AI life cycle effectively.
- **Intellectual property:** As AI becomes more sophisticated and "creative", key legal issues in 2023 will include the concepts of "inventorship" and "patentability" of products created by, or using, AI as well as the provenance and ownership of data. Already we have seen divergence across jurisdictions in approaches in this area, with fundamental impact on the granting of rights to third parties and the successful commercialisation of such products and software.
- **Contracting for AI:** Businesses are increasingly recognising that contracts for AI procurement, development or investment are a crucial part of the wider AI governance process. When contracting with suppliers or entering into a collaboration for AI development, there will be increased focus on case-by-case assessment in order to negotiate appropriate terms to address the non-deterministic nature of AI, to manage supplier risk exposure and to allocate clearly rights, responsibility and liability. For the same reasons, such contracts will increasingly be spotlighted in due diligence exercises prior to investment or M&A transactions.

For more, see our international expert panel discussion: Managing AI in an evolving legal landscape.

4

Emerging regulatory frameworks for digital assets, services and markets

The power and real-world consequences of digital content, interactions and assets are more evident than ever before. Countries around the world are introducing regulation designed to protect consumers, promote data sharing, safeguard competition and manage the digital playing field. Courts are applying existing legal principles to new technologies. In 2023, we will see rapid evolution of the legal frameworks for the regulation of digital services, online content, digital assets and digital markets.

What's next?

- **Online services and content:** Governments and law makers are focused on tackling unfair or harmful practices, dark patterns, disinformation, and the risk of deepfakes and other technologies being weaponised to manipulate people. From the recently introduced EU Digital Services Act and China's laws on deep synthesis technology, to the UK Online Safety Bill and the proposed US Kids Online Safety Act, we will see significant, if fragmented, progress in regulating an array of online services and technologies.
- **Cloud computing and Internet of Things (IoT):** The proposed EU Data Act seeks to grant users rights to access and port data generated by IoT products and contains controversial proposals designed to facilitate switching between cloud providers that could have significant impact on competition in these markets, as well as ramifications for database rights and complex interplays with privacy laws. Market studies by competition authorities in Europe and Asia are considering competition in relation to cloud services. These services are also in the spotlight in the context of proposed EU and UK resilience standards applicable to so-called 'critical third parties'.

- **Digital Markets:** Antitrust authorities are continuing to focus on regulation of the digital sphere and have their sights set on curtailing the power of the largest players in the digital markets. The EU's Digital Markets Act (DMA) entered into force last year, and in 2023 we will begin to see which companies are designated gatekeepers and how aspects of the legislation will be implemented. The DMA is part of a global trend in tackling the regulation of competition in digital markets – with legislation at varying stages in the US, the UK, Australia, China and Korea. The year ahead will give a better picture of the degree of divergence in approach between jurisdictions as these laws develop. We will also see significant investigations and litigation as prominent companies come under scrutiny for alleged anti-competitive behaviour connected with their use of technology and data.
- **Digital assets:** In the wake of the failure of key players in the crypto-asset ecosystem and as regulatory expectations for managing operational and other risks arising from uses of distributed ledger technology are maturing, regulators around the world will increasingly require more stringent risk controls as they focus on the resilience of firms holding exposures to cryptoassets. There will be an increase in disputes surrounding digital assets; it is likely that we will see court decisions shaping how insolvency proceedings, securities laws and duties of care apply in relation to digital assets, as well as further court rulings on the concept of 'property' in relation to non-fungible tokens or NFTs.

For more, see Fintech Trends 2023; Crypto Litigation & Arbitration - Trends to Watch in 2023; The Data Act: A proposed new framework for data access and porting within the EU; The Digital Services Act – What is it and what impact will it have? and The Digital Markets Act: A new era for the digital sector in the EU.

Part 2 – Tech Markets and Supply Chains

Digital Worlds

5

Recent metaverse exploration has often focused on immersive virtual worlds where consumers interact through an avatar. In 2023, other potential use cases for immersive digital worlds are expected to develop more quickly than the consumer-focused metaverse; the "industrial metaverse" will come to the fore. Digital worlds will remain big business for entertainment, however, with video games more popular than ever and esports viewership on the rise.

What's next?

- **Industrial metaverse:** The application of metaverse technologies to industrial use cases has the potential to be transformative for operational efficiency and facilitating research across sectors. Augmented and virtual technologies combined with robotics can enable experts to perform tasks in an immersive environment with real-time data while operating at a distance from the asset being repaired or the patient being treated. Virtual representations of physical properties or machines – "digital twins" – can enhance their real-world operation and efficiency, as well as allow for potential changes to their operation to be simulated before being implemented in the physical world. Companies, private investors, governments and law-making bodies are paying attention: China has released a four-year "Virtual Reality and Industry Application Integration Development Action Plan", South Korea plans to invest in a metaverse ecosystem as part of its 'digital new deal' and the EU is expected to publish its metaverse strategy later this year.
- **Gaming and e-sports:** Expect increased investment and collaborations in gaming and esports as their popularity continues to grow. We will see new brands entering the space and collaborating with established companies and teams. Wearables and augmented or virtual reality technologies will be increasingly incorporated, and we will see a rise in mobile-specific games and tournaments. We will also see increased protection of players, consumers and competition – including a focus on player welfare, greater regulation of in-game purchases and loot boxes, scrutiny on processing of personal data and sustained attention from antitrust authorities.

For more, read: Level Up: A Legal Guide to the Video Games Industry and The metaverse: risks and opportunities for businesses.

6

Changing markets and supply chain challenges

Shifting economic conditions will bring changes in deal-making activity in 2023. We will see strategic consolidation through bolt-on acquisitions and business co-operation, as well as an uptick in carve-out transactions. This year we will also see a focus on strain in the technology supply chain. Today's businesses have more complex technology stacks with multiple points of potential supplier failure, and the trend for businesses to rely on supplier-controlled cloud solutions and to engage growth businesses for core technologies means that supply chain distress can have significant ripple effects.

What's next?

- **Tech M&A:** We will see increased use of targeted due diligence, tailored contractual mechanisms and creative planning to get deals done quickly in shifting market conditions or to seize time-sensitive opportunities. These will include increased use of indemnity protections, 'earn-out' mechanisms, post-close due diligence tests and remediations, employee retention pools and equity rollover packages. Adjusted due diligence will focus on technology and data as key growth drivers and dependencies, as well as on supply chain risk and resilience.
- **Tech supply chain distress:** There will be scrutiny on potential distress in the tech supply chain. Financially robust businesses will be looking to transform in response to an increased focus and requirement for ongoing and long-term operational resilience. They will be building systems and processes to manage disruptive issues that could impact business continuity, such as cybersecurity and supply chain risk.
- **Carve-out transactions:** With the growth in the value of data as an asset, we will see a lot of transactions selling businesses with significant data sets. As well as some sales by necessity, we will see real opportunities to unlock value. As the target is often fully integrated with the seller, negotiations will centre on technology separation issues, rights to control data and intellectual property.
- **Consolidation:** We will see increased collaboration through consolidation as companies come together to combine resources, technology and expertise for greater efficiency, innovation and growth. This will include consolidation of fintech platforms, particularly in the digital trade space. We may also see more disputes in relation to collaborations in 2023 where changes in market demand, competitor activity, and legal frameworks strain existing partnerships, or where regulatory action occurs.
- **Digital assets:** Recently we have seen how volatile the digital asset ecosystem can be. As fallout continues from last year's raft of collapses of crypto exchanges, investors and miners, we will see a continuation of investor class actions, challenges to arbitration agreements, and satellite litigation from bankruptcy and insolvency proceedings. Going forward, we will see greater due diligence into counterparties and potential acquisition targets, as well as a move from more established market participants away from volatile products in favour of increasingly sophisticated distributed ledger technology (DLT) financial markets infrastructure projects.
- **Digital capital markets:** We will see continued exploration of how DLT might transform the issuance, trading and settlement of debt securities and the development of regulatory initiatives to stimulate the use of DLT in financial services. Expect a number of projects under regulatory pilot regimes and sandboxes, and a global increase in digital bond issuances.

7

Digital protectionism around strategic technology

Certain technologies will see significant investment activity and cross-sector collaborations and consolidations – including crucial components and infrastructure that underpin digital connectivity, and technologies that support energy transition goals. The critical nature of such technologies has not escaped governmental and regulatory notice. We will continue to see forms of digital protectionism that use legislation to stimulate or protect certain industries or technologies, both boosting and complicating transactions and other agreements relating to these technologies.

What's next?

- **Net-zero tech:** A combination of climate change imperatives, energy security concerns and technology sovereignty policies means markets are seeing a radical uplift in investments and transactions relating to technologies for energy transition. In the US, the Inflation Reduction Act is using huge subsidies to expand domestic manufacture of clean energy, batteries and electric vehicles, and reduce dependence on imports. The EU has responded by announcing its "Green Deal Industrial Plan", which will facilitate subsidies for green industries. These investments are being mirrored, and exceeded, by private finance as green technology businesses are attracting increased private equity and other investments. Energy transition targets (such as the UK's combustion engine ban by 2030) are also playing a role in driving traditional industries, such as automotive and power, to transform their business models. These businesses are pursuing partnerships and collaborations with companies that can provide technology or license intellectual property that support their transformations. Among the legal considerations for investments and transactions in this sector will be foreign direct investment controls, antitrust laws and the EU's new Foreign Subsidies Regulation, which enters into force in Q3 2023.
- **Semiconductors:** The semiconductor supply chain has seen a turbulent few years, from the global chip shortage, to increasing protectionism, to blocked and aborted deals. Reliable chip supplies are critical for a wide range of sectors, including automotive, consumer goods, healthcare and national infrastructure. Cross-border M&A and foreign direct investment are subject to increasing scrutiny worldwide, primarily driven by competition, national security and industrial policy concerns. In 2023 (and beyond) we will see this critical industry being shaped by M&A and strategic partnerships, vast public subsidies, regulatory interventions, antitrust and intellectual property law, and the EU Foreign Subsidies Regulation.

For more, see our webinar: M&A and regulations reshaping global semiconductor supply and our articles Semiconductors - Increasing governmental and regulatory scrutiny and New Bargaining Chips: US Department of Commerce Imposes New Export Controls on the Semiconductor Industry and Imposes Changes to the UVL and Entity List.

- **Investment treaties:** Alongside increased government intervention in investments in certain technologies, changing policies around data use, digital regulation and ESG requirements are significantly impacting a number of business models – including in relation to cloud computing, digital assets, data centres and digital advertising. At the same time, the number of tech-related disputes being brought by overseas investors against states under investment treaties has steadily grown. Investors are turning to investor-state arbitration to seek redress in relation to governmental actions or omissions that have had a significant impact on the viability of an investment. In 2023 we will continue to see foreign investors engaging in investor-state dispute settlement and considering the availability of treaty protection prior to making significant investments in another jurisdiction. Larger players may even be able to negotiate direct agreements with host states, providing recourse to investor-state arbitration.
- **Space Tech:** As well as public funding, we are seeing increased private investment, finance and partnerships as many governments are changing legislation to encourage entrepreneurship and access to investments in the space industry. Those exploring space tech opportunities will need to navigate carefully laws arising from digital sovereignty agendas, including regulations on the sale of restricted technology, heightened requirements for operational resilience, ESG concerns and complex supply chains.

For more, see our webinar Space Tech – investment opportunities and our articles, Space Tech: Challenges and Opportunities and The Space Race: Regulatory requirements for space launch and transmission in Australia.

8

Telecoms connectivity and digital infrastructure

With unprecedented levels of content consumption and 'connected things' across increasingly diverse locations, ubiquitous and resilient internet connectivity has never been more important. There will be continued investor interest in traditional digital infrastructure classes – fibre optics, towers and data centres – as well as pioneer investors looking for novel opportunities in adjacent technologies, use cases and infrastructure.

What's next?

- **Increased regulatory controls for data centres:** Data centres will continue to come under the microscope of regulators as they consider the environmental, planning, data protection and national and global security issues that data centres present.
- **Key focus on ESG opportunities:** While especially relevant for power-hungry data centres, ESG issues and opportunities will remain a central consideration for many digital infrastructure investments in 2023. Private communications networks, for example, provide the vital underpinning infrastructure for energy-efficient smart buildings, smart cities and next-generation power generation and transmission infrastructure.
- **Beginnings of Alt-Net consolidation:** Space for "fibre to the premises" (FTTP) building alternative network providers (alt-nets) is starting to reach saturation point in many large markets. We will see consolidation driven by the current economy climate. With the assets still possessing sound fundamentals, opportunities will exist for well-positioned operators and investors.
- **Complexity in FTTP deployments and legacy networks:** Consumer expectation of broadband service quality is increasing and legacy technologies are starting to lag behind the reality of FTTP deployments. We expect to see deals involving complex commercial arrangements dealing with the short- to medium-term coexistence of these technologies.
- **Consolidation in towers market:** With the 'towerco' model rapidly reaching maturity in its current form in many markets, we expect to see consolidation as tower operators seek scale to justify investment in meaningful operational improvement initiatives and to hedge against revenue-risk resulting from customer consolidation through M&A activity, the deployment of OpenRAN, and resource sharing technologies.
- **Change in regulatory approach:** Scale is becoming essential for survival for the most critical part of the industry. We will see sector and completion regulators alike working out how to adapt their traditional thinking and approaches to facilitate continued growth while protecting consumer interests.

For more, see our Digital Infrastructure Webinar Series and our briefing Data centre financings: what's next?

CONTACTS

Devika Kornbacher
Partner
New York
T: +1 212 878 3424
E: devika.kornbacher@cliffordchance.com

Jonathan Kewley
Partner
London
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com

Paul Landless
Partner
Singapore
T: +65 6410 2235
E: paul.landless@cliffordchance.com

Dessislava Savova
Partner
Paris
T: +33 1 4405 5483
E: dessislava.savova@cliffordchance.com

Rita Flakoll
Global Head of Tech Group Knowledge
London
T: +44 207006 1826
E: rita.flakoll@cliffordchance.com

Zayed Al Jamil
Partner
London
T: +44 207006 3005
E: zayed.aljamil@cliffordchance.com

Yong Bai
Partner
Beijing
T: +86 10 6535 2286
E: yong.bai@cliffordchance.com

Neil Barlow
Partner
New York
T: +1 212 878 4912
E: neil.barlow@cliffordchance.com

Jennifer Chimanga
Partner
London
T: +44 207006 2932
E: jennifer.chimanga@cliffordchance.com

André Duminy
Partner
London
T: +44 207006 8121
E: andre.duminy@cliffordchance.com

Steven Gatti
Partner
Washington DC
T: +1 202 912 5095
E: steven.gatti@cliffordchance.com

Megan Gordon
Partner
Washington DC
T: +1 202 912 5021
E: megan.gordon@cliffordchance.com

Jack Hardman
Partner
Dubai
T: +971 4503 2712
E: jack.hardman@cliffordchance.com

Ling Ho
Partner
Hong Kong
T: +852 2826 3479
E: ling.ho@cliffordchance.com

Nelson Jung
Partner
London
T: +44 207006 6675
E: nelson.jung@cliffordchance.com

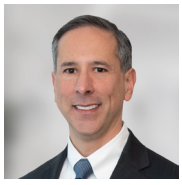
Nadia Kalic
Partner
Sydney
T: +61 2 8922 8095
E: nadia.kalic@cliffordchance.com

Renée Latour
Partner
Washington DC
T: +1 202 912 5509
E: renee.latour@cliffordchance.com

Vanessa Marsland
Partner
London
T: +44 207006 4503
E: vanessa.marsland@cliffordchance.com

Claudia Milbradt
Partner
Dusseldorf
T: +49 211 4355 5962
E: claudia.milbradt@cliffordchance.com

Josep Montefusco
Partner
Barcelona
T: +34 93 344 2225
E: josep.montefusco@cliffordchance.com



Peter Mucchetti
Partner
Washington DC
T: +1 202 912 5053
E: peter.mucchetti@cliffordchance.com

Michihiro Nishi
Partner
Tokyo
T: +81 3 6632 6622
E: michihiro.nishi@cliffordchance.com

Dieter Paemen
Partner
Brussels
T: +32 2 533 5012
E: dieter.paemen@cliffordchance.com

Simon Persoff
Partner
London
T: +44 207006 3060
E: simon.persoff@cliffordchance.com

Sharis Pozen
Partner
Washington DC
T: +1 202 912 5226
E: sharis.pozen@cliffordchance.com

Stephen Reese
Partner
London
T: +44 207006 2810
E: stephen.reese@cliffordchance.com

Gunnar Sachs
Partner
Dusseldorf
T: +49 211 4355 5460
E: gunnar.sachs@cliffordchance.com

Katrin Schallenberg
Partner
Paris
T: +33 1 4405 2457
E: katrin.schallenberg@cliffordchance.com

Kate Scott
Partner
London
T: +44 207006 4442
E: kate.scott@cliffordchance.com

Benjamin Sibbett
Partner
New York
T: +1 212 878 8491
E: benjamin.sibbett@cliffordchance.com

Daniel Silver
Partner
New York
T: +1 212 878 4919
E: daniel.silver@cliffordchance.com

Thomas Voland
Partner
Dusseldorf
T: +49 211 4355 5642
E: thomas.voland@cliffordchance.com

Samantha Ward
Partner
London
T: +44 207006 8546
E: samantha.ward@cliffordchance.com

Joachim Fleury
Consultant
London
T: +44 207006 8050
E: joachim.fleury@cliffordchance.com

Jaap Tempelman
Senior counsel and co-head of Tech Group
Amsterdam
T: +31 20 711 9192
E: jaap.tempelman@cliffordchance.com

Gail Orton
Head of EU Public Policy
Paris
T: +33 1 4405 2429
E: gail.orton@cliffordchance.com

Phillip Souta
Head of UK Public Policy
London
T: +44 207006 1097
E: phillip.souta@cliffordchance.com

Julia Dreosti
Counsel
Sydney
T: +61 2 8922 8025
E: julia.dreosti@cliffordchance.com

Alexander Kennedy
Counsel
Paris
T: +33 1 4405 5184
E: alexander.kennedy@cliffordchance.com

Brian Harley
Consultant
Hong Kong
T: +852 28262412
E: brian.harley@cliffordchance.com

Peter Harris
Counsel
Tokyo
T: +81 3 6632 6635
E: peter.harris@cliffordchance.com

Michael Evans
Counsel
London
T: +44 207006 1757
E: michael.evans@cliffordchance.com

Kimi Liu
Counsel
Shanghai
T: +86 10 6535 2263
E: kimi.liu@cliffordchance.com

Andrea Tuninetti Ferrari
Lawyer - Counsel
Milan
T: +39 02 8063 4435
E: andrea.tuninettiferrari@cliffordchance.com

Laura Nixon
Knowledge Director
London
T: +44 207006 8385
E: laura.nixon@cliffordchance.com

Mark Fisher
Senior Associate
London
T: +44 207006 1480
E: mark.fisher@cliffordchance.com

Arun Visweswaran
Senior Associate
Dubai
T: +971 4503 2748
E: arun.visweswaran@cliffordchance.com

Shruti Hiremath
Senior Associate
London
T: +44 207006 3075
E: shruti.hiremath@cliffordchance.com

Herbert Swaniker
Senior Associate
London
T: +44 207006 6215
E: herbert.swaniker@cliffordchance.com

Chris Grey
Senior Associate
London
T: +44 207006 4984
E: chris.grey@cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

Clifford Chance, 10 Upper Bank Street, London, E14 5JJ

2302-004667