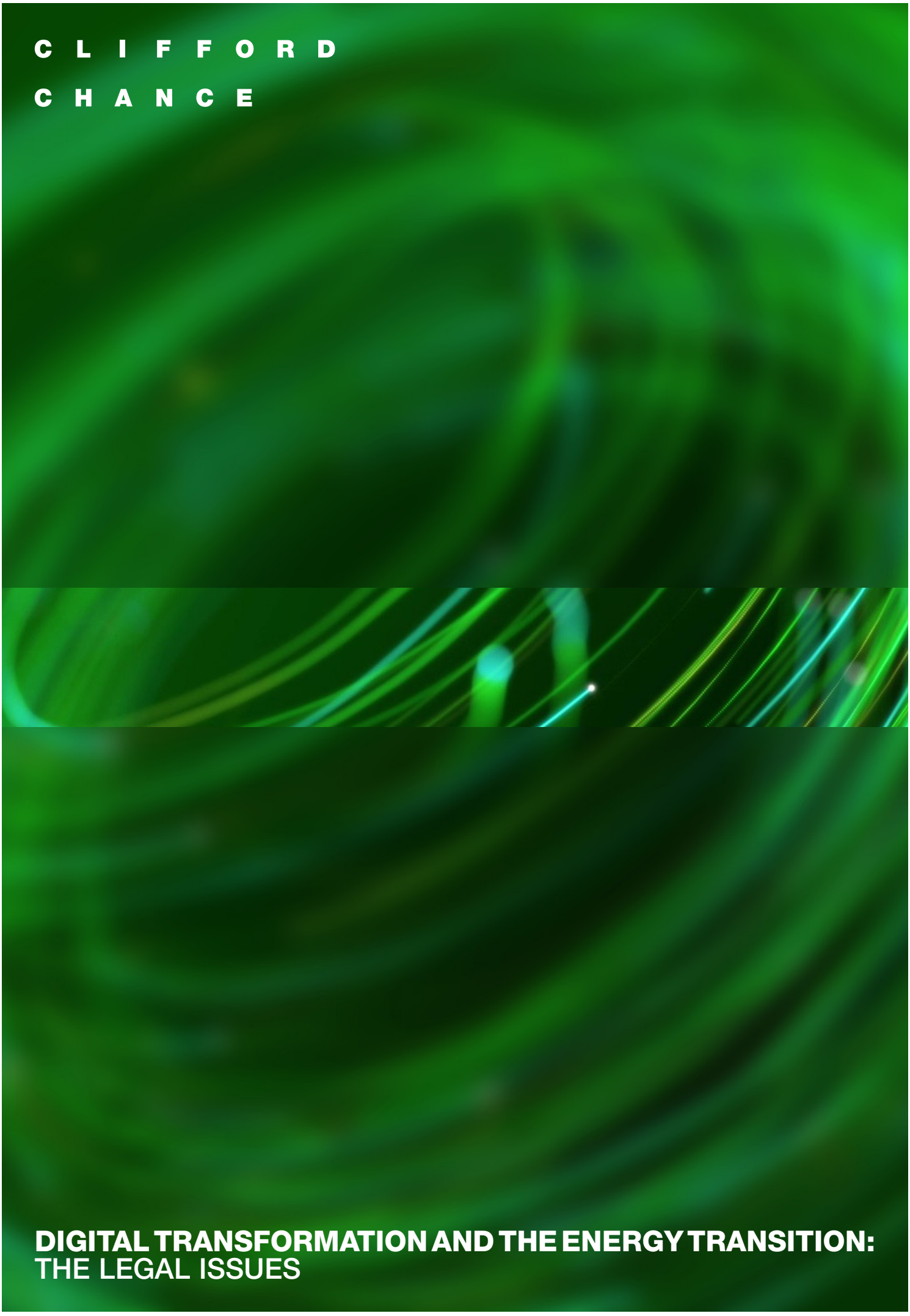
CLIFFORD

CHANCE



DIGITAL TRANSFORMATION AND THE ENERGY TRANSITION: THE LEGAL ISSUES

DIGITAL TRANSFORMATION AND THE ENERGY TRANSITION: THE LEGAL ISSUES

The twin challenges of the energy transition and digital transformation are closely linked, with each playing a crucial role in the success of the other. On the one hand, digital transformation is helping us reduce our carbon footprint in a variety of ways, be it through video calls, new forms of mobility or the real-time monitoring of how much energy we are using at home. On the other hand, we need to ensure that those technologies do not consume more energy than they need to and are subject to appropriate governance.

The energy transition is underpinned by a broad digital transformation in relation to the way our energy is generated, distributed and used. The proportion of renewable energy we generate is increasing year on year and a long overdue digital transformation is occurring in the retail energy sector. AI and other sophisticated software are being used to optimise smarter distribution networks. Cybersecurity and the protection of personal data have become critical as the adoption of smart meters and electric vehicles (EV) accelerates. Protecting the IP arising in respect of innovative net zero technologies, including software, is now as important in the energy sector as it is in other more traditionally "software-centric" sectors.

This briefing will examine some of the legal considerations arising from the relationship between the energy transition and digital transformation in these contexts.

The scale of investment is starting to meet the scale of the net zero challenge

Achieving the Paris Agreement's objectives of delivering net zero by the middle of the century and limiting the impact of climate change will be among the greatest challenges of our age.[1]

Many public and private companies, particularly in the US and Europe, have made pledges in support of these ambitions,[2] and legislation[3] related to achieving (and in some cases reporting on) net zero progress is incentivising more companies to develop or invest in green technologies to achieve their net zero and sustainability commitments. This trend is likely to accelerate considering increased regulatory and advertising standards intervention in relation to greenwashing[4] and related public scrutiny.

1 See the Paris Agreement under the United Nations Framework Convention on Climate Change. "Net zero" refers to a state in which the level of anthropogenic greenhouse gas emissions into the atmosphere is balanced by their removal from the atmosphere.
2 According to the United Nations Framework Convention on Climate Change, 8,307 companies, 595 financial institutions and 65 healthcare institutions are among the 11,309 non-state actors that have announced net zero commitments as of September 2022.
3 According to the Energy and Climate Intelligence Unit's Net Zero Tracker, Canada, Chile, Denmark, the EU, Fiji, France, Germany, Hungary, Ireland, Japan, the Republic of Korea, Luxembourg, New Zealand, Nigeria, Spain, Sweden and the UK are among the countries that have signed net zero commitments into law, with China, the US and the UAE being among the nations with net zero goals reflected in policy documents.
4 See, for example, the European Commission's proposed Directive on the substantiation and communication of explicit environmental claims (the Green Claims Directive) and our briefing on the new ISSB Sustainability Disclosure Standards.

The 2022 US Inflation Reduction Act has proven to be another catalyst for change. The Act designates USD369 billion in subsidies for companies who invest in and develop net zero and low-carbon intensity technologies (see our briefing: Inflation Reduction Act of 2022). The EU has responded in kind, with its Green Deal Industrial Plan for the Net Zero Age and the 2023 Net Zero Industry Act – with the intention of stimulating investment and growth in specific green technologies including batteries, solar, wind power, heat pumps and renewable hydrogen (see our briefing: The European Net Zero Industry Act). Similar packages have been proposed elsewhere, including in the UK, where the 2023 Spring Budget allocated substantial investments in carbon capture technologies and small modular reactors, and in Japan, where the GX (Green Transformation) Promotion Act – enacted in May 2023 – aims to accelerate decarbonisation in Japan through introducing a carbon pricing scheme and issuing energy transition bonds to support investment in net zero technologies.

VW Group's recent decision to carefully consider whether to construct a vast new battery plant in the US or Eastern Europe is expected to be heavily influenced by the support available in each jurisdiction and highlights the political significance of green technologies at a time when energy security and sovereignty are attracting unprecedented attention. For more, see our paper: The Green Industrial Policy Revolution – developments in trade, energy transition and geopolitics.

In addition to the flow of public capital, recent years have seen significant growth of energy transition investment funds and other forms of 'responsible' private investing. The popularity of these funds is attributable to private investor appetite for ESG credentials and enthusiasm to capitalise on the anticipated growth in renewable energy generation, and the emergence of new, globally scalable, low-carbon technologies. In particular, the volume of assets exhibiting ESG-related credentials under management of signatories to the UN Principles of Responsible Investing has grown from USD21 trillion in 2010 to USD121 trillion in 2021. In practice, the International Energy Agency (IEA) estimates that investment in clean technologies is on course to reach USD1.7 trillion in 2023 – with investments in solar technologies eclipsing investments in oil production for the first time in history. The think tank, Atlas Public Policy, estimates that, to date, USD830 billion has been invested in vehicle and battery plants and battery recycling facilities. (See our briefing: Betting on batteries: powering the clean energy transition.)

These investor preferences toward sustainable businesses and an increasing sense of urgency to fulfil net zero and sustainability commitments are also gaining momentum as a driver in private M&A. Just as investors recognise the long-term financial benefits of 'green' assets, potential acquirers, from private equity firms to longer-term investors, are drawn to these opportunities. Relatedly, we expect to see significant changes in capital allocation and capital flows, including divestments of high-carbon assets.

Digital transformation has taken centre stage in the energy transition

Digital technologies can be central to solving energy transition challenges. For example, smart energy distribution hardware, deployment of increasingly sophisticated software platforms in retail energy, use of AI to predict demand, leveraging digital twins to maximise power plant efficiencies, and the application of blockchain technology to monitor and validate renewable energy supply, are just a few examples of digital transformation in this space.

The increased role of digital technology as an 'enabler' of the energy transition means that related areas of law are becoming more important than they were before within affected sectors. These include:

- **Data Governance and Commercialisation:** the collection, processing and sharing of personal data and other valuable datasets from smart meters and IoT-enabled domestic devices will be key to successfully leveraging distributed energy resources. Over time, individual domestic and commercial energy customers are likely to play contributory roles as utilities pursue grid resilience and consumption optimisation goals. For example, we already see retail energy providers managing domestic EV charging loads to avoid times of peak demand by using data collection techniques and flexible tariffs to incentivise customers to charge their EVs at times when networks experience reduced loads. Ensuring consumer trust in relation to these use cases through effective and transparent data governance will be key to ensuring that these data remain available for processing, analytics and innovation. Data governance is also expected to play an increasing role in reducing the environmental impact of cloud workloads as companies examine the sustainability of long-term storage of unused data.
- **Cybersecurity and Resilience:** ensuring that the grid and its connected assets are technically secure and resilient to cyber threats will be a priority. Energy security is essential in an increasingly volatile geopolitical environment. The proliferation of connected devices (including in the home) may create access points or other vulnerabilities as energy resources become increasingly interconnected. More broadly, today's businesses have more complex technology stacks with multiple points of potential vulnerability or supplier failure. These risks arise at a time when cyber risk and operational resilience is a growing priority for legislators, with both horizontal and sector-specific laws affecting sectors such as energy, mobility and digital infrastructure.
- **AI and Machine Learning:** increasingly sophisticated software systems and platforms are playing critical roles, including through streamlining energy services, enabling smart girds and effective workload consolidation and scheduling in data centres. The regulatory framework that applies to these systems – particularly where they fall within emerging definitions of 'AI systems' – is complex and evolving.
- **Contracting for Digital Transformation and Protecting IP:** digital transformation and efficiency are fundamental to the transition to net zero. With the introduction of renewables and distributed energy resources, alongside the expected increase in demand for electricity arising from the electrification of mobility, grid infrastructure will need to evolve to institute more control over supply and demand. As capital is invested in innovative technologies, the IP arising in respect of those innovations will need to be protected. Research partnerships will be forged, and the universe of applicable technology regulation will continue to expand. As innovators seek to commercialise their IP, their contractual risk will also need to be carefully managed – in respect of their supply chains and in respect of any licensing terms imposed on their customers. On the other hand, licensees will also be looking for robust contractual protections as they deploy potentially transformative innovations within their businesses.

Legal challenges: perspectives from different sectors

What role is digital technology playing as industries focus on their net zero ambitions, and what legal challenges are they facing?

Retail Energy and the Smart Home

In many parts of the world, the retail energy sector has been under pressure from wholesale price rises, strict regulation (including price caps in the UK and Singapore) and a wide range of geopolitical events. Many players have concluded that digital transformation is the only way to reduce the cost-to-serve customers in the face of shrinking margins. These transformations are often enabled by software and other technologies that can automate customer service and data collection, integrate and manage distributed assets (for example, battery storage, EV chargers, heat pumps and solar panels) and permit and enable smart tariffs.

With the adoption of new software platforms (e.g. to manage customer relationships or to manage domestic smart energy devices), legal challenges arise in connection with the processing of collected data, managing vendor and customer interfaces, contracting and IP risk. Where software platforms are critical to the durability and resilience of energy services, licensees may expect the reassurance of source code escrow deposits and strict service levels. Other challenges arise in connection with increasingly popular software continuous integration and continuous delivery methodologies (i.e. CICD), with customers increasingly unable to perform traditional acceptance testing in respect of CICD software, particularly where new source code deployments are 'pushed' directly to the licensees' local instances or cloud environments many times each day.

More broadly, there has been no let-up in EU legislative activity affecting digital services – with, for example, the recent finalization of the Data Act, the adoption of the Data Governance Act and the revised Network and Information Systems (NIS2) Directive, and a common European energy data space in progress. Specific cross-sector EU legislation on AI is edging towards finalisation too, which could have an impact on the way in which AI systems are deployed to predict energy demand and manage distributed resources (see our article: EU AI Act: Final negotiations can begin after European Parliament vote).

Cybersecurity is crucial to the resilience of energy supply. This is reflected in both legislation and in contractual terms between energy retailers and IT service providers. For example, the EU's NIS2 Directive further harmonises Member State laws on cybersecurity for critical infrastructure by imposing enhanced requirements for "essential" or "important" entities, including those in the retail energy sector. Together with its implementing EU Member State laws (which are to follow), it obliges businesses operating in the EU to adopt specific cybersecurity risk management processes and comply with strict reporting standards, in each case with a view to operating resilient systems and services (see our briefing: NIS 2 Directive: Europe revamps its cybersecurity framework). Similarly, the Singapore Cybersecurity Act 2018 imposes obligations on owners of a critical information infrastructure (CII) supporting the delivery of an 'essential service' across prescribed sectors, including the energy sector. CII owners must comply with mandated codes of practice and performance standards, conduct cybersecurity audits and risk assessments, and share certain information with the Cyber Security Agency of Singapore where requested. Likewise, in the US, the Cybersecurity and Infrastructure Security Agency (CISA) provides oversight and a

regulatory framework on cybersecurity measures that must be taken by various "critical infrastructure" owners and operators, including in the energy sector. For example, the CISA published cross-sector cybersecurity performance goals to provide a baseline set of best practices and a benchmark for critical infrastructure operators. The CISA also works with other US regulatory agencies, like the Transportation Security Administration (TSA), to develop additional industry-specific cybersecurity requirements, such as the latest TSA Security Directive on oil and natural gas pipeline cybersecurity requirements which mandates the submission of cyber assessment plans and reports to the TSA by owners and operators.

Through the Data Act, the EU recognises the role of data access in driving innovation, and potentially improving operational efficiency (see our briefing: EU Data Act: Political Agreement Reached). The wider EU Data Strategy adopted in 2020 sets out the related idea of establishing a single EU market for data based on common European data spaces. To facilitate data sharing and improve the interoperability of data, these EU-wide data spaces are to be developed in several strategic sectors – including energy, with the stated ambition of supporting the EU's energy sector goals.

Data sharing frameworks to support a European data space for energy were laid out in the Data Governance Act, adopted by co-legislators in May 2022 (see our article: An overview of the EU Data Governance Act). Although the aim of the proposal is to facilitate data reuse, the conditions imposed on the exchange of non-public data have been criticised as creating additional hurdles, with definitions that are imprecise and provisions that could allow, for example, the blocking of transfers of valuable non-personal data to countries outside the EU. Procuring data, particularly from private organisations, can also be prohibitively expensive, particularly for new market entrants. An evolving trend to facilitate data access and sharing includes using application programming interfaces (APIs) to democratise data flows, through standardised data transfer technology. The energy industry will face a new wave of commercial and contracting issues in realising the benefit of using API marketplaces. Issues include pricing of data points shared via APIs, integration considerations and delivering frictionless customer experiences.

Finally, retail energy companies also realise that they could see value erosion unless they own or control parts of the EV ecosystem and many are investing in their related domestic and public offerings. Retail energy providers with supply arms also recognise that they need to invest in renewable generation as old plant is taken offline. These businesses must also balance the capital expenditure of their investments in the regulated retail space with the capital demands of their upstream and downstream businesses – which may drive transformative M&A as these businesses evolve their strategic ambitions for growth.

Data Centres and Cloud Computing

Whilst the use of cloud computing and related data centre infrastructure underpins many innovative net zero technology solutions, especially the effective management of distributed energy resources (such as battery storage and virtual power plants), the cloud and data centre sector is subject to its own green revolution.

That revolution is a crucial one since, according to a European Commission study, data centres were responsible for 2.7% of the EU's entire electricity demand in 2018. Other

studies suggest that data centres are currently responsible for the same percentage of global greenhouse gas emissions as the global airline industry. Energy consumption by data centres is set to increase in the next decade as new data-hungry technologies such as AI, virtual reality and autonomous driving take hold, and 5G networks drive greater consumption of data. These new technologies will require new data centres to be built locally to deliver the low latency required to support them. This involves processing data nearer to where it is collected or created with a view to enabling near real-time analytics to be performed and to minimise outages or interruptions (see our briefing: Data Centre Trends 2023). Given the anticipated growth in demand and increased legislative and commercial pressures regarding sustainability, data centres will need to dramatically improve efficiency and reduce (or offset) carbon emissions by using renewable energy and other means.

In Europe, the European Commission ambitiously asserts that the sector should be carbon neutral by 2030 and is urging data centre operators to take appropriate steps to achieve this goal, despite growing demand. To this end, the European Commission has issued a Code of Conduct for Data Centre Efficiency featuring a series of steps for data centre operators to adopt. Singapore is similarly encouraging improved data centre efficiency, including through the Infocomm Media Development Authority (IMDA's) Green Data Centre Standard, which provides a framework and methodology designed to help organisations establish systems and processes to improve the energy efficiency of their data centres in tropical climates. The US has also set similar carbon neutral goals with President Biden's statement that the US will aim to significantly reduce greenhouse gas pollution by 2030 with a goal of having a net zero economy by 2050. The US has also applied this broader net zero policy objective in the context of data centres. For example, the Environmental Protection Agency (EPA) has recently worked with global data centres to develop best practices and guidance to help data centre co-locations become more energy efficient, such as through airflow management and proper cabling, as part of the EPA's Energy Star program. In China, establishment of regional and nationwide data centres is a priority on government's agenda, with green energy sourcing and reduced energy consumption being part of the announced rationale regarding location of regional hubs.[5] China requires data centres to use renewable energy to the extent possible,[6] encourages participation in renewable energy market trades, and requires energy efficiency to be taken into account throughout the design and construction of data centres and monitored thereafter.[7] The largest customers of data centre operators are similarly focused on the energy transition: having announced their own sustainability targets, they are looking to their supply chain for help.

5 The "Eastern Data, Western Computing" plan was first introduced at the end of 2020 when the National Development and Reform Commission (NDRC), the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT), and the National Energy Administration (NEA) jointly released the Guiding Opinions on Accelerating the Construction of a National Integrated Big Data Center Collaborative Innovation System. Since then, several policy documents have been released to support plans for further development of China's data centres including, in February 2022, approvals from NDRC for the construction of four regional hubs.

6 For example, see China's Central Commission for Cybersecurity and Informatization's 14th Five-Year Plan for National Informatization, issued on 28 December 2021.

7 In 2021, MIIT issued a three-year target for data centres to achieve power usage effectiveness ("PUE") (see MIIT's notice on the Three Years' Development Plan for New Data Centres (Year 2021 – 2023) dated 4 July 2021). At the regional level, under the Implementation Opinion on Accelerating the Construction and Development of New Infrastructure (Year 2020 - 2025), Shenzhen municipal government also sets out specific PUE requirements for small-middle size data centres.

Digital technologies are increasingly being explored in improving energy efficiency and/or sourcing renewable energy in the context of data centres and cloud computing. For example, with a significant proportion of data centre energy use being related to cooling and ventilation, machine learning is being used to optimise 'white space cooling' and limit energy use to where it is needed. It can also assist with consolidating workloads and enabling and disabling circuits in line with need. Beyond reducing energy consumption, digital technology can also play a role in enabling data centres to source renewable energy supply – blockchain can be used to establish the provenance of renewable energy resources, including by allowing real-time time-stamping at the point of energy generation to give transparency of energy origin.

As data centre owners and operators seek to reduce their energy consumption for political and legislative reasons, as well as to reduce operating costs, they should pay close attention to their procurement and customer contracts. Supply and procurement contracts related to the installation of electrical equipment including power delivery units and redundancy systems should be scrutinised carefully owing to the mission criticality of the underlying hardware and the importance of their efficiency. Where suppliers are licensing software to operators and owners that are intended to balance loads across servers or allow real-time monitoring of servers and services, it will be important to carefully consider the cyber security commitments offered by those suppliers – particularly where cyber-attacks can be just as effective at taking a data centre offline as a power outage. For both equipment and software, suppliers' performance claims and service levels must be carefully considered to minimise the probability of severe exposure to customer claims in the event of power cuts, hardware failure, cyber incidents or similar events.

Data centre operators and owners must also pay close attention to their power usage effectiveness[8] data since these data are increasingly scrutinised by existing and prospective customers who are keen to meet their own ESG goals (as well as by interested third parties, including NGOs). Relatedly, operators and owners must pay attention to the claims they might make in their marketing and advertising materials, given the advertising standards and other regulatory scrutiny that can be brought to bear in relation to misleading or disputable claims.

Data governance also plays an increasing role in reducing the environmental impact of cloud workloads. Although moving applications to hyperscale data centres can itself achieve a reduction in energy usage, the sustainability of moving existing workloads into the cloud on an 'as-is' basis is increasingly being queried. As the volume of unused data that is stored by businesses increases, strategic data governance programmes that reduce digital waste are more important than ever in enabling companies to meet legal requirements (for example, under data protection laws), manage data risks through minimising unnecessary processing and reduce the environmental impact of their operations.

8 PUE was published in 2016 as a global standard under ISO/IEC 30134-2:2016.

Data centres (and cloud computing, more broadly) are crucial to the operations of most companies and financial institutions. Whilst the emerging legislative[9] and political drivers will continue to incentivise data centre owners and operators to embrace technologies in pursuit of net zero, it is also clear that their customers' ESG goals will catalyse change – and those operators who can demonstrate progress in these areas will likely achieve a significant competitive advantage.

Mobility

The automotive and aviation industries have been at the forefront of many technological innovations. The competitive imperative to innovate is, more recently, being supercharged by political intervention. In Europe, this includes the prospective UK ban on the sale of new ICE vehicles from 2030, the imposition of cross-fleet emissions standards across the EU, and the recently agreed EU regulation on sustainable aviation fuels (the "ReFuelEU Aviation Initiative"). The US also continues to promote digital innovation through an evolving regulatory landscape for mobility, including through tax preferential treatment policies to encourage relevant automotive technology R&D.

OEMs are investing unprecedented sums in R&D,[10] with a particular focus on EV-efficiency technologies including solid-state and other higher energy density batteries, e-fuels and hydrogen fuel cells. In addition, automotive and aviation businesses are seeking collaborations instead of, or in addition to, conducting their own R&D to gain access to new technologies and/or market share. These mobility solutions are supplemented by innovation in the fields of connectivity, infotainment, advanced driver-assistance aids, and AI-enabled route planning. Connectivity is at the core of a modern car and the car is arguably now as much a "connected" device as a smartphone – with data from its sensors being shared between vehicles, infrastructure and other IoT-connected devices. All these innovations, collaborations and procurement arrangements generate regulatory, contractual, privacy, and IP protection and enforcement issues in relation to their development, acquisition and/or integration.

New functionality is increasingly digitised with a view to new modes of income generation including connected vehicle services, subscription services and targeted, individualised customer experiences. On the one hand, these digital services may offset some of the major capital expenditure on mobility-related R&D. On the other hand, some of these digital services are necessary to enable a more customer-centric experience that can overcome some of the challenges associated with e-Mobility. For example, as EVs proliferate, connected services that consolidate invoicing in relation to the use of charging infrastructure operated by different providers may reduce some of the challenges associated with destination and 'en route' EV charging stops (as well as driving further revenues for OEMs, charging network providers and other over-the-top providers). Also, over-the-air software updates can avoid the need for more costly repairs and prolong the life of vehicles, with resulting sustainability advantages.

9 For example, see the draft German Efficiency Act (which specifies PUE targets for Data Centres that will be effective from 2027) and the energy efficiency requirements introduced by the UK's Amended Building Regulations dated June 2022.

10 European R&D spend increased by 75 percent between 2011 and 2019, US OEM spending over the same period grew by 30 percent to €13 billion, and Asian carmakers increased their spend by 33 percent to €28 billion according to PWC Strategy& Germany's report: Digital Automotive R&D, 2020.

Traditional sector-specific regulations focusing on cars continue to target safety but with OEMs expanding their ecosystems and legislators watching technological advances in mobility carefully, more areas of regulation will become relevant. Laws on cyber security and the protection of personal data already catch OEMs in most modes of customer-facing activity. For example, China maintains a focus on the regulation of mobility data and, in addition to cross-sector laws such as the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law, has been issuing various national standards applicable to mobility. In the EU, the General Data Protection Regulations will apply to many customer-related data processing activities, alongside more specific guidelines such as the EDPB's Guidelines 1/2020 on the processing of personal data in the context of connected vehicles and mobility-related applications. In the US, recently enacted data privacy laws and regulations across multiple states, such as the California Privacy Rights Act and the Virginia Consumer Data Protection Act, will also apply to connected vehicles and mobility solutions in the consumer context, including with respect to the collection and processing of GPS data.

Upcoming cross-sector digital regulations such as the EU AI Act, EU Data Act (affecting, amongst other things, the sharing of data from "connected products") and the EU Cyber Resilience Act (affecting cybersecurity requirements for products with digital elements) will also catch numerous elements of the modern automotive or air mobility ecosystems, from sharing GPS data, to route planning, to AI-enabled predictive maintenance, to establishing software security standards. With so much data now being collected, generated and processed by vehicles, aircraft, drones and their OEMs, the mobility industry will need to keep pace (see our briefing: The Data Act: A Proposed New Framework for Data Access and Porting within the EU).

In addition, new targeted legislative frameworks are in progress in certain jurisdictions to address the evolving use of digital technologies in the mobility sector. For example, Germany has passed a law on highly automated and autonomous driving, the EU has enacted harmonised regulations on civil drones (impacting a broad range of drones, including passenger drones) and, in the UK, the government has announced plans to develop a new legislative framework to allow for the wider rollout of autonomous vehicles by 2025 (see our article: Rollout of autonomous vehicles: UK government plans for a legislative framework).

In summary, the mobility sector is transforming as it adapts to new laws and explores evolving technologies. There remains significant growth potential as the industry pursues new avenues of innovation, such as the shift towards EVs and alternative fuel (for example, e-fuels and fuel cells, or sustainable aviation fuels) – along with parallel developments in autonomous and connected technologies.

AUTHORS

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

Holger Lutz
Partner
Frankfurt
T: +49 69 7199 1670
E: holger.lutz@cliffordchance.com

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

Jane Chen
Senior Associate
Beijing
T: +86 10 6535 2216
E: jane.chen@cliffordchance.com

Sian Smith
Senior Associate
Tokyo
T: +81 3 6632 6320
E: sian.smith@cliffordchance.com

Ricky Legg
Associate
Houston
T: +1 202 912 5943
E: ricky.legg@cliffordchance.com

CONTACTS

Stella Cramer
(Tech/Digital)
Partner
Singapore
T: +65 6410 2208
E: stella.cramer@cliffordchance.com

André Duminy
(Tech/Digital)
Partner
London
T: +44 207006 8121
E: andre.duminy@cliffordchance.com

Jennifer Chimanga
(Tech/Digital)
Partner
London
T: +44 207006 2932
E: jennifer.chimanga@cliffordchance.com

Kelly Gregory
(Corporate Group)
Partner
Shanghai
T: +86 21 2320 7234
E: kelly.gregory@cliffordchance.com

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

Jonathan Kewley
(Tech/Digital)
Partner
London
T: +44 207006 3629
E: jonathan.kewley@cliffordchance.com

Devika Kornbacher
(Tech/Digital)
Partner
Houston
T: +17138212818
E: devika.kornbacher@cliffordchance.com

Anthony Giustini
(GFM)
Partner
Paris
T: +33 1 4405 5926
E: anthony.giustini@cliffordchance.com

Ling Ho
(Litigation & Dispute Resolution)
Partner
Hong Kong
T: +852 2826 3479
E: ling.ho@cliffordchance.com

Lena Ng
(Financial Regulation)
Partner
Singapore
T: +65 6410 2215
E: lena.ng@cliffordchance.com

Michael Pearson
(Energy & Infrastructure)
Partner
London
T: +44 207006 4753
E: michael.pearson@cliffordchance.com

Thomas Voland
(Energy & Infrastructure)
Partner
Düsseldorf
T: +49 211 4355 5642
E: thomas.voland@cliffordchance.com

Phillip Souta
(Tech/Digital)
Global Director of Tech Policy
London
T: +44 207006 1097
E: phillip.souta@cliffordchance.com

Herbert Swaniker
(Tech/Digital)
Senior Associate
London
T: +44 207006 6215
E: herbert.swaniker@cliffordchance.com

Rob Donell
(Real Estate)
Senior Associate
London
T: +44 207006 1110
E: rob.donell@cliffordchance.com

Adam Hunter
(Tech/Digital)
Lawyer
London
T: +44 207006 1499
E: adam.hunter@cliffordchance.com

Robert Clay
(Innovation / Create)
Head of Product Ideation and Exploration
London
T: +44 207006 1137
E: robert.clay@cliffordchance.com

Eleanor Hooper
(Knowledge &Thought Leadership)
Knowledge Director
London
T: +44 207006 2464
E: eleanor.hooper@cliffordchance.com

CLIFFORD

CHANCE

Any content herein relating to the PRC is based on our experience as international counsel representing clients in business activities in the PRC and should not be construed as constituting a legal opinion on the application of PRC law. As is the case for all international law firms with offices in the PRC, whilst we are authorised to provide information concerning the effect of the Chinese legal environment, we are not permitted to engage in Chinese legal affairs. Our employees who have PRC legal professional qualification certificates are currently not PRC practising lawyers.

This publication does not necessarily deal with every important topic or cover every aspect of the topics with which it deals. It is not designed to provide legal or other advice.

www.cliffordchance.com

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

© Clifford Chance 2023

Clifford Chance LLP is a limited liability partnership registered in England and Wales under number OC323571

Registered office: 10 Upper Bank Street, London, E14 5JJ

We use the word 'partner' to refer to a member of Clifford Chance LLP, or an employee or consultant with equivalent standing and qualifications

If you do not wish to receive further information from Clifford Chance about events or legal developments which we believe may be of interest to you, please either send an email to nomorecontact@cliffordchance.com or by post at Clifford Chance LLP, 10 Upper Bank Street, Canary Wharf, London E14 5JJ

Abu Dhabi • Amsterdam • Barcelona • Beijing • Brussels • Bucharest • Casablanca • Delhi • Dubai • Düsseldorf • Frankfurt • Hong Kong • Houston • Istanbul • London • Luxembourg • Madrid • Milan • Munich • Newcastle • New York • Paris • Perth • Prague • Rome • São Paulo • Shanghai • Singapore • Sydney • Tokyo • Warsaw • Washington, D.C.

Clifford Chance has a co-operation agreement with Abuhimed Alsheikh Alhagbani Law Firm in Riyadh.

Clifford Chance has a best friends relationship with Redcliffe Partners in Ukraine.

2307-007237