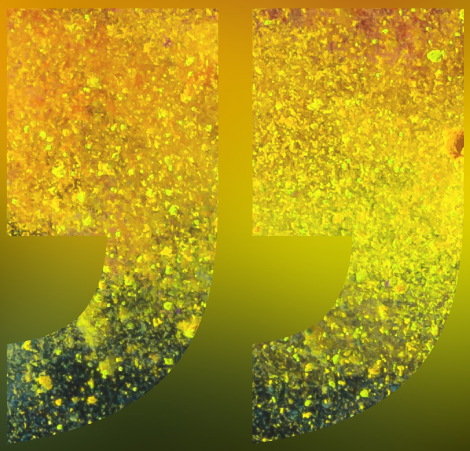
CLIFFORD
CHANCE

TECHNOLOGY AND THE ENERGY SECTOR
FOUR TRENDS TO WATCH AND FOUR CHALLENGES



— THOUGHT LEADERSHIP

APRIL 2018

TECHNOLOGY AND THE ENERGY SECTOR
FOUR TRENDS TO WATCH AND FOUR CHALLENGES

Technology is transforming the energy sector. It's driving efficiency, cutting costs and helping energy companies to better understand their customers, but that transformation comes with a number of challenges. Our experts outline the trends that will have a significant impact on the industry and the legal risks to watch out for.

FOUR TRENDS TO WATCH

Artificial intelligence

The energy sector is investing heavily in AI for a potentially wide range of uses, including:

- Thermal power generation – to improve efficiency in turbine burners by incorporating AI technology into the fuel distribution process.
- Renewable power generation – analysis of wind and operational data to increase production by reducing the impact of high wind hysteresis effects.
- 'Smart' technology – machine learning is being used for monitoring energy efficiency and consumption (smart meters) and in electricity transmission and distribution, to balance supply and demand (smart grids).
- Upstream oil and gas – to improve accuracy when identifying locations for drilling, and to optimise drilling operations (e.g. using data on flow rate, pressure and vibration and combining this with environmental information).

What are the risks?

- Algorithmic bias: The growth of AI has significant legal and ethical implications. AI tools make unpredictable decisions and can be biased where the underlying data it uses is skewed. There is a risk that by using AI tools, energy companies may inadvertently engage in anti-competitive, unethical or market abusive behaviour. Where AI is used in large systems such as electricity grids, the consequences of any failures are magnified.
- Inadequate regulatory frameworks: Given the speed with which new technology is introduced, it is unsurprising that rules and regulations lag behind. This is a real concern in highly regulated energy markets and carefully balanced energy systems (power and gas grids in particular). There is a risk that regulatory frameworks are insufficiently flexible or otherwise unfit for purpose to allow the full benefits of new technologies to be realised. Of at least equal concern is the risk that they are unable to prevent abuse or mitigate market shocks (such as price spikes) when technology allows decisions to be taken quicker than rules and regulators can respond.
- Antitrust: There is a likelihood of increased oversight and regulation as the law and regulators catch up with the technology; this may include increased scrutiny of antitrust implications, for instance if there is a concentration of systematically important AI suppliers which creates natural monopolies/oligopolies.

Blockchain (Distributed Ledger technology, DLT)

Numerous companies are currently developing blockchain applications for the energy sector, though none of these have moved beyond the concept or pilot stage yet. Possible applications include:

- Decentralised energy distribution – one trial, run in New York in 2016, involved off-grid-generated energy being sold directly from one neighbour to another through a blockchain system.
- Smart contracts – blockchain makes it possible for energy networks to be controlled through smart contracts, which would signal to the system when to initiate transactions.
- Electricity usage and supply forecasting – Elia, Belgium's electricity transmission system operator, has been exploring the use of big data blockchain to construct better forecasting models.

Improved forecasting has a direct impact on decisions regarding grid investments and sizing of grid tariffs, managing the maintenance of lines and substations, prevention of grid congestion and the sizing of so-called 'ancillary services' (balancing reserves).

What are the risks?

- Jurisdiction and applicable law: Where servers are decentralised and can be spread around the world, pinpointing where a breach or failure occurred (and taking the appropriate cross-border action) may be complex. In the UK, the Financial Markets Law Committee (FMLC) has just published a paper on this subject, emphasising the need to develop an international conflict of laws framework for DLT applications and recommending solutions that could be adopted.
- Enforceability of smart contracts: There are currently many open questions across jurisdictions as to the extent to which smart contracts are legally effective and enforceable.
- Transparency: As blockchain is trialled as a possible replacement for traditional trading contracts, issues of transparency and regulation are never far away.

Big data

Energy companies are increasingly capturing, storing and analysing the data generated by their day to day operations with a view to cutting costs, improving efficiency and reducing risks and downtime. Examples include:

- Upstream oil and gas – analysing seismic data to predict where oil may be found, and using data to predict which equipment may fail and replacing it before it does.
- Electricity generation – using data to ramp flexible assets up and down in response to real and near-real time supply and demand forecasts.
- Utility companies – advanced analytics are being used for a variety of purposes, including reducing procurement costs and managing vegetation along power lines, preventing outages through accurate predictions about when to replace equipment, or responding to an outage in real time, and helping utilities better understand customers and their energy use. This knowledge can then be used to design new products and services.

What are the risks?

- Data protection: Privacy laws apply if big data contains any personal information such as names, addresses, health records, bank details or unique identifiers. The obligations of organisations dealing with such data, and the associated compliance risks, have been further magnified by the new EU GDPR regime (see below).
- Accuracy of datasets: Data from publicly available sources, from other businesses, or collated by the business itself, may contain errors. These errors may then be included in trend analysis and predictions on which the business depends for strategic and investment decisions.

Robotics and autonomous vehicles

Robots and drones are already widely used in the energy industry, particularly for inspecting difficult-to-access locations such as offshore risers and surveying pipelines and subsea infrastructure. As the use of robotics becomes more widespread and sophisticated, so new legal and commercial issues arise. Looking a little further ahead, the expected transformation of the transport sector with the move towards both electric vehicles and autonomous vehicles will give rise to a raft of new challenges for the sector.

What are the risks?

- Liability: Robotics raise a number of difficult questions – if a robot malfunctions and causes damage to property or the environment, who is liable? The manufacturer? The company that deployed it? A range of approaches is under discussion across jurisdictions, including those based on strict liability (no fault required) and risk management (liability of a person who was able to minimise the risks). Companies in the energy sector will need to be aware of these developments and respond accordingly.

- Antitrust: Is joint or pooled licensing allowed? Would selling cars at a price materially below market value in order to collect necessary data, but which also keeps out new entrants, be a breach of antitrust laws? If agreements are properly structured then such risks can be minimised, but it will be important for companies active in this area to keep on top of market and regulatory developments.

FOUR CHALLENGES

Cyber security

The World Energy Council has warned that increasing interconnection and digitisation of the industry makes it a prime target for cyber criminals, state-sanctioned cyber attacks, terrorists and hacktivists. A large scale attack on energy infrastructure could trigger economic and financial disruption, loss of life and massive environmental damage. Regulators across the globe are responding by putting greater responsibility for cyber security on the energy industry.

Recent developments in the EU include:

- Smart metering – in November 2016, the European Commission published a proposal stating that all consumers should be entitled to request a smart meter from their supplier. This has boosted the take-up of smart metering across the EU. The Commission also published a cybersecurity package which proposed greater scrutiny of software and other components used to monitor industrial control systems. These requirements will be relevant for smart meter providers.
- EU Security of Network and Information Systems Directive (NIS Directive) – this directive must be transposed by EU Member States into local law by 9 May 2018. It places new obligations on operators of essential services (including energy firms) to ensure the cyber security measures they have in place are appropriate. While it has been left to member states to determine the precise details on a nation-by-nation basis, the UK implementation will likely cover areas such as identity and access control; service protection; data and system security; and staff awareness and training. In addition, firms face new incident reporting obligations, not only in the context of cybersecurity incidents but also potentially in respect of physical incidents affecting the security of network and information systems. Fines for non-compliance are likely to be onerous.

Data privacy

Energy companies hold a vast amount of customer data, including highly sensitive information such as payment details. This data is stored in multiple places including operational systems, CRM systems, data warehouses, analytical datamarts, big data environments and documents. Recent advances in energy management such as smart grids, are introducing a further level of complexity into data management for energy companies.

Consumers need clarity and reassurance about how their energy consumption data can be accessed, by whom and for what purposes, and about the choices they have to opt out of data sharing. Accordingly, as energy companies start collecting greater volumes of personal data, they must ensure that they are complying with global data privacy regulations.

The EU General Data Protection Regulation (GDPR) comes into force on 25 May 2018. It seeks to modernise EU law on personal data and at the same time introduces a raft of stricter rules on data security. Significantly, the GDPR will bring with it increased reporting and compliance burdens for companies within the energy sector who hold significant amounts of personal data including:

- Enhanced rights for data subjects.
- A broader extra-territorial scope.
- New sanctions – regulators can impose fines of up to 4 per cent of global turnover (or EUR 20 million, whichever is higher).

Intellectual assets

Advances in technology, particularly around renewable energy, and a surge in oil and gas production in the last few years means that the number of patents issued to energy companies has increased substantially and the number is expected to rise.

All businesses with potentially valuable IP must be alive to:

- Protecting value: Where a business amasses large, valuable IP portfolios on which its proprietary processes are reliant, it is essential to ensure that adequate IP protections are in place to guard against potential infringement by competitors.
- Patent assertion entities/non-practising entities (NPEs): The risk posed by NPEs is growing. NPEs obtain the rights to one or more patents in order to profit by means of licensing or litigation, rather than by producing their own goods or services. A recent study by the Boston Consulting Group has shown that NPEs are increasingly targeting the energy industry, with a steady increase in the number of lawsuits brought by NPEs against energy companies.

Tech M&A

Energy firms are increasingly investing in, or acquiring, tech start-ups to bring expertise 'in-house' and it's a trend that looks set to continue. According to a study by Mergermarket, the number of mergers and acquisitions across the technology, media & telecom (TMT) sector reached an all-time high in 2017, with 3,389 deals worth a combined US$498.2 billion. The volume of acquisitions has also increased, with CB Insights finding the number of AI start up acquisitions growing fivefold, from 22 in 2013 to 115 in 2017. Within the energy sector alone, a 2017 study by accountancy firm BDO found that mergers and acquisitions involving energy companies and AI start-ups soared in average value from around $500 million in the first quarter of 2017 to $3.5 billion in the second quarter.

M&A of technology companies, particularly the smaller ventures that are common in the industry, brings specific considerations, including:

- Identification of assets/value: The question of what is actually being sold/purchased is key. Often third parties, whether licensors, developers, founders, employees or others, claim licences to or other rights in algorithms, code, trade secrets and other key intellectual property. Securing robust invention assignment agreements from all past and current contractors and employees is critical, among other protections, to assure the buyer is receiving all that has been paid for.
- Purchase price consideration: The consideration for the acquisition can also be complex. Many purchases in this space will tie the eventual consideration to factors such as customer sales, EBITDA or other objective benchmarks, and can involve complicated earn-out mechanisms.
- Due diligence: Performing due diligence on target tech companies can be challenging. Many are early-stage businesses founded by young and inexperienced entrepreneurs and often do not have proper record-keeping processes in place or understand the importance of maintaining paper trails. This creates a sizeable task for the buyer as it tries to assess the risks involved in the acquisition.

Our M&A Trends 2018 report contains further detail and additional factors to consider for tech M&A deals. The report can be found on our Global M&A Toolkit.

CONTACTS

Clifford Chance's dedicated tech and energy sector teams are working together to help our energy clients navigate these tech issues. Please get in touch with any of the key contacts listed below to discuss any of the matters highlighted in this paper.

TECHNOLOGY

Jonathan Kewley
Partner
London
T: +44 20 7006 3629
E: jonathan.kewley@cliffordchance.com

André Duminy
Partner
London
T: +44 20 7006 8121
E: andre.duminy@cliffordchance.com

Stephen Reese
Partner
London
T: +44 20 7006 2810
E: stephen.reese@cliffordchance.com

Samantha Ward
Senior Associate
London
T: +44 20 7006 8546
E: samantha.ward@cliffordchance.com

Jennifer Mbaluto
Senior Associate and Co-Head of East Africa
London
T: +44 20 7006 2932
E: jennifer.mbaluto@cliffordchance.com

Jamie Andrew
Lawyer
London
T: +44 20 7006 1367
E: jamie.andrew@cliffordchance.com

Dessislava Savova
Partner
Paris
T: +33 14405 5483
E: dessislava.savova@cliffordchance.com

Claudia Milbradt
Partner
Düsseldorf
T: +49 21 1435 55962
E: claudia.milbradt@cliffordchance.com

ENERGY

James Pay
Partner
London
T: +44 20 7006 2625
E: james.pay@
cliffordchance.com

Ashvin Seetulsingh
Partner
London
T: +44 20 7006 8635
E: ashvin.seetulsingh@
cliffordchance.com

Nicholas Hughes
Partner
London
T: +44 20 7006 4621
E: nicholas.hughes@
cliffordchance.com

Graham Phillips
Partner
London
T: +44 20 7006 2354
E: graham.phillips@
cliffordchance.com

Joanna Lilley
Professional Support Lawyer
London
T: +44 20 7006 4488
E: joanna.lilley@
cliffordchance.com

Richard Tomlinson
Partner
Paris
T: +33 14405 5216
E: richard.tomlinson@
cliffordchance.com

Florian Mahler
Partner
Düsseldorf
T: +49 21 1435 55232
E: florian.mahler@
cliffordchance.com

Hein Tonnaer
Partner
Amsterdam
T: +31 20711 9528
E: hein.tonnaer@
cliffordchance.com

CLIFFORD

CHANCE

www.cliffordchance.com

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

J20181403182143