A SUSTAINABLE FUTURE
WILL SMART ENERGY GET US DER?

Alexander Dittel of Wedlake Bell LLP discusses the benefits and risks of harnessing smart energy data, and the current regulatory framework.

The COVID-19 pandemic accelerated digital transformation by several years, including the modernisation of supply chains. According to a global survey by McKinsey & Company published on 5 October 2020, digital technologies, monitoring devices, analytics software and digital marketplaces have matured to enable organisations to support weak points in their supply chains, anticipate breakdowns, build safety stock and use multiple suppliers (*www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/how-covid-19-has-pushed-companies-over-the-technology-tipping-point-and-transformed-business-forever*).

A parallel can be drawn with smart energy. What started as a technology that empowered consumers to understand their consumption, moderate usage habits and eliminate estimated billing, is now fast evolving to address the current energy crisis. Smart energy promotes renewables in the fight against climate change and limits dependence on foreign fossil fuel-based energy, an issue that is often leveraged in international politics. As geopolitical events work overtime to push the UK and Europe towards decarbonising the energy supply chain, it is becoming a priority to gain access to detailed consumption data, develop predictive analytics and connect new renewable energy sources to the grid. There is hope that smart energy will get us there.

This article discusses the benefits of harnessing smart energy data and data sharing, the privacy and cyber risk concerns in relation to smart energy, and how it is regulated.

SMART ENERGY

The basic idea of smart energy is that an understanding of energy consumption can help to optimise supply and achieve grid stability (*see box "The basics of energy supply"*). Sudden changes in the load on the grid can cause changes in voltage and frequency, and even a power generator failure and resulting outages. Forecast algorithms have been essential in replacing the traditional top-down monitoring of the grid and tackling, for example, the recent rebound of energy demand to above pre-COVID-19 pandemic levels. Data also allows the grid to identify faults quickly, restore power after outages and focus investment on critical infrastructure.

In addition, modern smart energy technologies enable smaller power generators, so-called distributed energy resources (DER), such as households with solar panels or businesses with onsite generators, to contribute their excess energy to the grid. Gas is slowly giving way to a fully electric future. Consumers have the option to install durable lithium ion-based batteries in their homes. There is also talk about vehicle-to-grid technology, where

electric vehicles (EV) are used to manage the intermittency of renewables by storing excess solar power generated by DER and selling it to the grid during peak demand. This is possible thanks to smart metering and sophisticated management software tackling the underlying data science problems, the resolution of which is key to a smart energy future.

However, the so-called "internet of energy" is more than this. In addition to infrastructure and energy generation assets, it plugs new players into the smart data stream, which can provide useful insights and services for the public benefit as well as improved commercial products. For example, smart energy can be used to:

- Inform households how they can save money on energy bills.
- Provide an early warning of an elderly resident falling or being incapacitated.
- Detect a faulty appliance in the household.

Without exaggerating, the potential of smart energy data is vast and unpredictable. The headlines about privacy concerns that have dominated the news in the past are giving way to reports of how data can fix today's energy challenges and increasing fuel poverty. This comes at a time when the UK's electricity consumption profile is changing significantly with the proliferation of EVs. However, the question still remains whether this objective outweighs data protection concerns.

Smart meters

Smart meters are connected devices that measure energy consumption onsite in households, commercial properties and other premises. The government launched its smart meter initiative, Smart Metering Equipment Technical Specification version 1, or SMETS1, in 2011 to help households stay in control of energy bills and reduce estimation in billing. The second version, SMETS2, is more sophisticated, more compatible for use with various consumer access devices and comes with ambitious objectives. The UK is hoping to transform the energy sector to tackle climate change and achieve net-zero carbon emissions by 2050. To do so, every energy supplier must accomplish a quota of smart meter installations each year. Following the pandemic lockdown, this programme resumed in full and over 52% of all meters, or around 29.5 million, are now smart, with the goal of reaching 100% by 2025 (*https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1077592/Q1_2022_Smart_Meters_Report.pdf*).

The Data Communications Company (DCC) maintains the smart meter data infrastructure, with utility companies being responsible for installations (*see box "Key players in the smart energy sector"*). In a household, the smart meter speaks to the home area network (HAN), which then sends the data through a communications hub to DCC's wide area network (WAN) operated by a telecoms provider. DCC then licenses the data to the energy supplier and other eligible users. Consumers will generally receive an in-home device from their energy supplier to monitor their consumption straight from the HAN. They can also connect a consumer access device.

In 2012, the government put in place the data access and privacy framework (DAPF), which is monitored and enforced by Ofgem, in order to regulate access to smart meter data held by DCC (*https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/43046/7225-gov-resp-sm-data-access-privacy.pdf*). The DAPF gives consumers access to their data and allows them to choose to share their consumption data with third parties every month, day or 30 minutes. Smart meters collect low frequency data every 30 minutes, which is necessary for billing and grid management. High frequency data is necessary to provide real-time information to the consumer for energy management and to enable automated

The basics of energy supply

Electric power is generated at power stations from fossil fuels, nuclear energy or renewable energy. In 2021, the top sources of electricity in the UK were:

- Gas, at 39.8%.
- Wind and solar, at 24.9%.
- Nuclear, at 14.9%.

According to the Department for Business, Energy & Industrial Strategy, electricity generated from renewable sources decreased by 9.3% between 2020 and 2021 due to less favourable weather conditions in 2021 (*https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1094025/UK_Energy_in_Brief_2022.pdf*).

The National Grid operates a high-voltage three-phase alternating current (AC) electricity transmission network, which is responsible for the bulk transmission of electricity across the country, from power stations to distribution substations. At substations, electricity is transformed to one phase lower voltage AC. The local distribution network operators, such as UK Power Networks, which owns electricity cables and lines across London, distribute power to consumers, including households. Before reaching its "near" final destination, power needs to be transformed to 230V at a frequency of 50Hz to be ready for consumption.

Organisations with a bigger demand may be connected directly to the higher voltage primary transmission level. Households with electric vehicles are recommended to switch to three-phase power instead of the standard one phase to build resilience that can meet the demands of electric vehicle charging and avoid blowing the fuse if there is not enough power onsite.

Electricity is sold to consumers by utility companies, such as British Gas, which buy it on the wholesale market. Unfortunately, many utility companies recently stopped trading due to the energy crisis, leaving only around 20 active suppliers on the UK energy market.

load control, which could be critical for high-demand households with EVs.

Most privacy concerns arise in relation to high frequency data. While household activity patterns can be inferred at a 30-minute temporal resolution, real-time data can identify which individual appliances are used in the household, or even which TV channel is being watched, based on fluctuations in demand.

DATA REGULATION

Access to smart meter data is subject to various industry rules, including:

- Gas and electricity supply licence conditions that apply to each licence holder, such as an energy supplier. The licence includes Ofgem's standards of conduct, including an overarching duty to treat customers fairly and have good customer outcomes in mind when accessing smart meter data (*www.ofgem.gov.uk/sites/default/files/docs/2019/02/licence_guide_standards_of_conduct_0.pdf*).

- The DAPF, which is enacted through supply licences.

- Smart meter communication licences, which the DCC grants to eligible users such as energy suppliers, distribution network operators and other public interest or commercial eligible users (*https://epr.ofgem.gov.uk/Content/Documents/Smart%20DCC%20Limited%20-%20Smart%20Meter%20Communication%20Consolidated%20Licence%20Conditions%20-%20Current%20Version.pdf*).

- The Smart Energy Code, which is enacted through DCC smart meter communication licences.

- The General Data Protection Regulation (*679/2016/EU*) (GDPR), which is now incorporated into the UK as the retained EU law version of the GDPR (UK GDPR). Under the UK GDPR, personal data, such as the Meter Point Administration Number (MPAN) and consumption data that relates to a household or sole trader, must be used in a transparent manner and justified under a lawful basis, such as contract, legal obligation, legitimate interest or consent (*see feature articles "GDPR enforcement: a changed landscape", www.practicallaw.com/w-030-5470 and "GDPR one year on: taking stock", www.practicallaw.com/w-020-0982*).

Key players in the smart energy sector

The key entities in the smart energy sector are:

- Ofgem, which regulates the smart energy sector.
- The Data Communications Company, which maintains the smart meter data infrastructure.
- The Department for Business, Energy & Industrial Strategy, which contributes to important policy decisions.
- Energy UK, which is a trade association for the energy industry and publishes guidance for the sector.

Access to smart energy data

Under the DAPF, licence holders must not request consumption data without consumer consent and appropriate transparency. Consumers must have a choice about:

- Temporal resolution of the data collected from the smart meter.
- Data sharing with other organisations.
- Using the data for sales and marketing purposes.
- How consumption data can be accessed to get the most benefit from it.

Despite relentless calls for the liberalisation of access to smart energy data, in its November 2018 review of the DAPF, the Department for Business, Energy & Industrial Strategy (BEIS) concluded that it remains fit for purpose (*https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/758281/Smart_Metering_Implementation_Programme_Review_of_the_Data_Access_and_Privacy_Framework.pdf*).

However, the introduction of half-hourly settlement (HHS) under the Smart Meters Act 2018, which is expected to be fully brought into force by 2025 through regulations made by the Secretary of State, will allow grid operators and energy suppliers to access half-hourly consumption data without consumer consent for the limited purpose of HHS. Ofgem's July 2018 data protection impact assessment concluded that, instead of an opt-in process, the opt-out route will ensure best uptake while still offering a choice to consumers (*www.ofgem.gov.uk/sites/default/files/docs/2018/07/data_protection_impact_assessment_2.pdf*). Ofgem confirmed its decision to proceed with market-wide HHS on 20 April 2021 (*www.ofgem.gov.uk/publications/electricity-retail-market-wide-half-hourly-settlement-decision-and-full-business-case*). Consumers can opt out from HHS and switch to daily readings instead. However, smart tariffs offering cheaper power at night are often conditional on HHS.

In addition, access to HHS data will be permitted for business readiness purposes, including forecasting, trading functions and the development of new products and services. Data used for these purposes must be anonymised and aggregated where practicable. Indeed, when inspecting the privacy notices of major energy suppliers, it is apparent that consumption data is used for analytics, product development and similar purposes on the basis of legitimate interest. This is slightly at odds with the industry's strict consent requirement and the UK GDPR.

In addition, distribution network operators (DNOs) will access smart meter consumption data without consumer consent to maintain an efficient and economic grid, and to comply with regulatory duties. However, every DNO must first have a privacy plan, approved by Ofgem, which sets out how data will be used and how it will be anonymised (*www.ofgem.gov.uk/publications/statutory-consultation-proposal-modify-condition-47-smart-metering-matters-relating-obtaining-and-using-consumption-data-slc-47-electricity-supply-standard-licence-conditions*).

In practice, organisations have found further ways to use smart energy data. Under their supply licence, organisations have to present a notice and obtain consent to process data in accordance with that notice. However, it could be argued that these broad consents are not compliant with the UK GDPR, which requires specific and informed consent and discourages bundling together multiple obscure purposes under one consent. In addition, many DNOs adopt the position that they are processing non-personal "system data", including monthly consumption data, maximum demand, voltage and export, the use of which allegedly is not subject to the DAPF or the UK GDPR. Others say that smart meter data accessed through consumer access devices, such as the supplier's dedicated app, are not subject to the DAPF. Anonymisation could also make it possible to share data with other parties outside of the regulatory framework.

Although there are ways to access such "derived" smart energy data, registering with DCC and obtaining consumer consent remains the most compliant way to tap straight to the source. While some licencees such as utility switching services may easily obtain consent for a service that has been requested and consented to by the consumer, some licencees, such as researchers, academia and public bodies may struggle to persuade the consumer to give consent (*see "Data research" below*). In addition, each user must take steps to verify that the consent does in fact come from the individual occupying the premises.

While this regulatory framework is rather complex, with an increasing number of energy-related apps and growing enthusiasm from consumers to monitor their usage, there may be a boom in add-on services similar to that flowing from open banking in the financial sector. BEIS is introducing a separate code for smart energy devices and schemes, which includes explicit consumer consent, data minimisation and encryption. However, organisations providing these devices and schemes are not subject to the DAPF and will have their own views on what amounts to good data protection under the UK GDPR.

Data flows are not limited to energy imports by consumers. A two-way data stream, including energy export data, is necessary to allow DERs to participate in the energy marketplace.

DISTRIBUTED ENERGY RESOURCES

DERs are small power generators. Households install DERs to reduce their energy bills and businesses install DERs to have backup power onsite in case of a grid outage. DERs include traditional generators, microturbines, wind turbines, solar arrays, battery energy storage systems and other systems that are often installed near load centres. However, DERs may produce excess energy at times and, without a large battery storage unit, this energy could go to waste. Smart energy solutions enable DER operators to sell their excess energy to the grid at prevailing rates.

For DERs to function, the following smart energy elements are required:

- Two-way smart metering to monitor power sold to the grid and to compensate the DER operator.
- Synchronisation of the frequency and voltage of the DER energy with the grid's standard 230V at 50Hz.
- Software to control the system.
- Aggregation virtual power plant software to give the DER access to the energy wholesale market.

While the excess output of one household or business would not assist with balancing the grid in any meaningful way, virtual power plants have emerged as aggregators that connect multiple or even hundreds of small DER operators at once to the energy market. These demand-side and supply-side smart energy software companies will access smart energy demand and export data through a DCC licence holder and by other means.

To support DER operators, the government launched a smart export guarantee in 2020 to guarantee payment for low-carbon electricity up to 5MW that is generated from solar photovoltaic, wind, micro-combined heat and power, hydro or anaerobic digestion.

While artificial intelligence (AI) and machine learning optimise power distribution through the grid and help customers to maximise the value of energy, energy storage is needed to make the most out of DER and renewables in general.

ENERGY STORAGE

Electricity is produced for a certain load on the grid. If the load increases, such as by a lot of homes using their air-conditioning at once, the frequency and voltage of the electricity could decrease. If the load suddenly reduces, the frequency goes up and so does the voltage. The speed governor at power plants regulates the speed of the generator to maintain a steady frequency and voltage in light of changes in the load. However, if these changes are significant, they could cause issues such as the power generator failing, equipment being damaged or fuses tripping.

There is never any excess electricity on the grid. Smart energy's predictive algorithms get better at output planning, which helps producers to generate only the power that is needed. However, particularly with renewables, excess electricity that is generated due to sunny or windy weather is harder to predict. The need for energy storage is a critical part of the UK's plan for a sustainable future based on renewable energy.

With advances in technology, there is a variety of lithium-ion battery units for residential and commercial use on the market. For example, a Tesla Powerwall 2 will support a household for 24 hours with its 13.5kWh capacity and 5kW output. The British Powervault 3 offers similar configuration options. These batteries are expected to remain at above 70% capacity during their ten-year warranty periods.

Battery energy storage systems allow consumers to store their DER energy, lower their energy bills, become independent from the grid and even sell energy back to the grid. Home batteries could be used to buy electricity when it is cheapest and store it for use when grid prices are more expensive, helping to lower household electricity bills.

According to an article published by Energy Storage News on 17 March 2022, at the industrial and infrastructure level, 446MW of battery energy storage was used in the UK in 2021 (*www.energy-storage.news/the-numbers-behind-the-record-breaking-rise-of-the-uk-battery-storage-market/#:~:text=Strong%20growth%20of%20installed%20capacity%20during%202021&text=The%20UK%20installed%20446%20MW,storage%20sites%20has%20also%20increased*). As reported by Solar

Media Market Research in their UK Battery Storage Project Database Report, more than 686 battery storage projects are underway to increase the current operational capacity for battery storage of 1.3GW to 4.5GW by the end of 2022 and 16.5GW in future (*https://marketresearch.solarmedia.co.uk/collections/solar-storage-research/products/uk-battery-storage-project-database-report*). The government is also investing in research to explore more durable and sustainable energy storage, and BEIS has awarded £6.7 million in funding for innovative longer duration energy storage projects (*www.gov.uk/government/publications/longer-duration-energy-storage-demonstration-programme-successful-projects*).

The use of batteries in smart energy is changing. The typical use of batteries is for their frequency response services to help balance the grid during critical events. For example, if a trip on the grid causes a frequency dip to 49.67Hz, batteries can produce a response output in milliseconds to restore the frequency to 50Hz. On the other hand, the use of batteries for energy trading is still exceptionally low. However, this may change in the future as more durable batteries enter the market.

Another technical challenge is measuring the charge of storage assets, which is volatile due to the nature of batteries. This makes long-term resource planning difficult. Nevertheless, with the sophistication of energy data analytics in the near future, energy storage is expected to enable renewable load shifting.

THE INTERNET OF ENERGY

The internet of energy is different from the internet of things in that, for security reasons, it relies on private networks, such as the DCC smart meter infrastructure, instead of public internet. However, some countries rely on public networks and face the security issues that come with it.

The modern metering of data flows, particularly with HHS, enable energy suppliers to incentivise customers to reallocate their consumption and benefit from cheaper off-peak tariffs; for example, EV owners can charge their car at night when wholesale energy prices are cheaper. On the other hand, some customers cannot escape peak-hour consumption and will prefer not to share their detailed consumption data.

Cyber risks of the internet of energy

In addition to its many benefits, the internet of energy increases cyber security risks; for example:

- Criminals could find valuable appliances to steal or determine the best time to commit a burglary.
- Service providers and retailers that buy charging network data to predict driving patterns and overall daily routines, or even estimate location based on an electric vehicle's (EV) mile range, could apply discriminatory pricing.
- Sensitive data about household activities could be inferred from household items such as fridges and washing machines, and be used, for example, for debt recovery.
- Data could be used for targeted advertising in a discriminatory way.
- Consent given on behalf of a household may not be reflective of the wishes of all of the occupants whose data is shared with other organisations.
- Smart energy companies could keep data for longer than expected, given the yet-to-be-unlocked increasing and unpredictable data analytics capabilities. This could increase the risk of a data breach.
- New smart energy products, such as home EV charging units, are often produced by start-ups with immature compliance with the retained EU law version of the General Data Protection Regulation (*679/2016/EU*) (UK GDPR) and which are not subject to a Data Communications Company licence and regulatory oversight. For example, load balancing sensors could be used to monitor the energy usage on premises to prevent a power cut but also be misused for other purposes, innocently or otherwise.
- Grid-edge technologies, such as fridges, could collect behavioural data, demographic data, usage data and contact information, purportedly based on consent which is not informed and is in breach of the UK GDPR.

Either way, consumers can connect a consumer access device in order to benefit from a number of new services based on energy usage data or make their data available to researchers for small rewards. In the near future, a large number of devices and apps will liberalise the way that consumers can use their consumption data. So-called "grid edge technologies", such as public EV charging stations, home chargers, connected white goods, EVs, and energy management apps may collect data outside of the smart meter infrastructure. However, giving access to data comes with risks; seemingly harmless data use could be used to influence daily life.

Non-intrusive load monitoring identifies the energy signatures of devices, events or activities. Apart from the ability to identify all individual appliances in the household, the data could be used for diagnostics; for example, detecting changes in the patterns of behaviour of individuals and enabling healthcare providers to predict those at risk of health conditions, such as Alzheimer's. As larger high-quality datasets become available, the accuracy with which such inferences can be made will increase; for example:

- Landlords could use usage or consumption data to verify compliance with the lease.
- Law enforcement agencies could identify suspicious activities or corroborate a testimony.
- Insurance companies could regulate premiums by monitoring trends in an insured's consumption data.

- Retailers could tailor their services based on customers' consumption habits.
- Manufacturers could develop new products designed for particular types of consumer.

Cyber risks

There are a number of obvious cyber risks with the internet of energy (*see box "Cyber risks of the internet of energy"*). The DCC network adheres to the cyber security standards set by the National Cyber Security Centre (*www.ncsc.gov.uk/information/the-smart-security-behind-the-gb-smart-metering-system*). The Network and Information Systems Regulations 2018 (*SI 2018/506*) impose security standards on the operators of critical infrastructure, including energy supply, energy transmission and networks, and smart meter networks (*see Briefing "Network and Information Systems Regulations: assessing the impact", www.practicallaw.com/w-018-7097*).

The Department of Energy & Climate Change and the Government Communications Headquarters (GCHQ) designed the smart metering system holistically with proportionate, practical security controls so that no single compromise can have a significant impact. However, due to the sophistication of attackers and the increasing potential for the misuse of energy data, vulnerabilities may continue to be exploited, particularly if smart energy data is collected outside of the regulated smart meter infrastructure.

Privacy-preserving techniques recently promoted in a briefing paper published on 26 May 2022 by the Energy Futures Lab institute of the Imperial College London offer solutions to many of these risks (*https://spiral.imperial.ac.uk/handle/10044/1/96974*). For example:

- User demand shaping that operates behind the smart meter can alter consumption patterns.
- With the use of a household battery, the smart control can hide particular characteristics that may be considered sensitive.
- Even without a battery, differential privacy can be used to introduce noise to provide mathematical guarantees of anonymity at the cost of reduced data utility.
- Homomorphic encryption enables data analysts to preserve data accuracy without accessing the underlying data, which is encrypted by way of arithmetic operations.
- Distributed learning can enable data utility while keeping data safely at device level.

DATA RESEARCH

Like other sectors, the smart energy sector is also aware of the significant opportunities in sharing data for analysis. Under the Digital Economy Act 2017, the Office for National Statistics can access energy usage data in fulfilling its statutory functions, including to produce official statistics and undertake statistical research that meets identifiable user needs for the public good. However, researchers, local authorities, consumer associations, climate activists and other parties should be able to access smart energy data, including personal data, in the public interest in order to drive the public benefits of research and statistics.

One data access initiative, which is operated by DCC and the Open Data Institute, seeks to explore how the combined sets of data generated by the internet of energy can be used to provide a range of services and products to consumers (*https://theodi.org/article/dcc-data-for-good-achieving-net-zero-through-smart-meter-data-access/*). For example, smart meter system data can potentially be used to help those suffering from fuel poverty. Many people are happy to consent to share data about themselves for societal benefits but want to understand and have a say in how it is used.

Under various initiatives, DCC already provides access to system data to various stakeholders for monitoring and research, and to data intermediaries for analytics. The government wishes to establish open data platforms. The Smart Meter Energy Data Repository is expected to offer access to smart energy data for purposes in the public interest, such as research (*https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1077685/Flexibility_Innovation_Programme_-_Smart_Meter_Energy_Data_Repository.pdf*).

Draft guidance published by the Information Commissioner's Office (ICO) in February 2022 (the draft guidance) on the research provisions within the UK GDPR and the Data Protection Act 2018 suggests that producing statistical research outputs based on anonymised data may be possible under the legitimate interest lawful basis for processing (*https://ico.org.uk/media/about-the-ico/consultations/4019614/research-provisions-draft-consultation-202202.pdf*). Research in the public interest could fall under the public task lawful basis. The research exemption does not apply if the intention is to use research results to make specific decisions about the data subjects or to target them with tailored services based on profiling. The draft guidance also stresses that it is not possible to switch from consent to another lawful basis if consent is withdrawn. This could jeopardise research efforts in industries with a prevalent reliance on consent, such as the smart energy industry.

While caution is in order, given the immaturity and low transparency of grid-edge technologies when it comes to data protection, the government's current pro-innovation stance may lead to a relaxation of these rules in the near future to enable further smart energy-related research (*see News brief "UK data protection reforms: towards a risk-based approach", www.practicallaw.com/w-036-3682*).

LOOKING AHEAD

Smart energy has matured over the last decade and taken on greater objectives. There is pressing public interest in advancing technologies that will lead to a future of responsible energy abundance, sustainable net-zero emissions and energy independence.

At the same time, most consumers still do not appreciate what information may be inferred from their energy usage data, while both legitimate and illicit exploitation possibilities of smart energy data are growing exponentially. It is clear that consent remains a strict but necessary requirement in the context of consumer lack of awareness and the unpredictable future application of smart energy data. This is contributed to by the so-called "black box problem" of AI, which means that it is uncertain what algorithms might infer from datasets and how this could affect individuals.

There are compelling arguments for unlocking the power of smart energy data.

Related information

This article is at practicallaw.com/w-036-7558

Other links from uk.practicallaw.com/

Topics

Data protection: general	topic/1-616-6550
Energy – environmental issues	topic/1-201-5565
ESG and sustainability	topic/w-032-4726

Practice notes

Compliance issues for energy suppliers	w-021-0413
Cybersecurity in the energy sector	w-014-5616
Electricity industry: overview	0-203-6634
Electricity licensing: overview	w-001-7766
Electricity storage: generation licensing framework	w-021-0654
Electricity storage: ownership and operation by network companies	w-022-8535
Electric vehicles and charging infrastructure	w-013-4404
Energy storage: overview	w-002-4852
Energy transition in the power sector: overview	w-031-9365
Ofgem: enforcement powers	w-010-2202
Ofgem: roles, powers and duties	w-002-4955
Renewable energy: overview	7-380-7949
Retail price capping in the energy sector	w-021-5329
Smart energy systems: overview	w-016-3023

Previous articles

EU regulatory data framework: a new generation (2022)	w-036-5428
ESG in a complex world: immaturity exposed (2022)	w-035-5886
ESG standards and ratings: know the score (2022)	w-035-4811
AI and automated decision making: to regulate or deregulate? (2022)	w-033-8467
EU regulatory data framework: a new generation (2022)	w-036-5428
AI and data protection: balancing tensions (2019)	w-020-9713

For subscription enquiries to Practical Law web materials please call +44 0345 600 9355

However, equally, there are concerns about a substantial number of market players with immature data protection compliance that can access data outside of the current regulatory framework, posing significant risks to consumers. The current regulatory framework is being amended to allow for access to data where it is needed in the public interest but, at the same time, the framework should be expanded to capture novel grid-edge processing activities.

Despite privacy notices that remain vague, consumer enthusiasm for consent could be sparked by the energy crisis in consumers' desperate search for a benefit or reward. Other than Ofgem's overarching objective to treat customers fairly, there is little to protect individuals from companies exploiting the current situation. Unless defeated by claims of anonymisation, the UK GDPR comes to the rescue but there has not yet been any enforcement action by the ICO, a regulator which promises to streamline the process of dealing with complaints by delegating back to the offending organisations.

It seems that the UK's current regulatory framework strikes the right balance between data utility and data privacy. Data sharing initiatives are well underway without much legislative activism. Having said that, the proposed Data Protection and Digital Information Bill anticipates wider access to customer data and business data, in a similar way to the significant Data Governance Regulation that is being introduced in the EU to benefit from data sharing for research and the public good (*see News brief "Data Governance Regulation: the wave of regulatory and competition reform begins", www.practicallaw.com/w-029-3479*).

Alexander Dittel is a partner in Technology at Wedlake Bell LLP.

