Lexis®PSL **TMT**

Internet of Things (IoT)—key legal issues

Jump to section

Show More

Produced in partnership with Matthew Hunt of Bristows and Pat Treacy of Bristows

The Internet of Things (IoT) is the term given to everyday objects (not just traditional computing devices, such as laptops and smartphones) which are connected to the internet. Other language used in connection with the IoT include: connected devices, smart objects, the internet of services, machine-to-machine (M2M) technology, sensor networks, the network of networks and pervasive computing or ubiquitous computing.

IoT can be applied to objects as diverse as running shoes, buildings, cars, fridge-freezers and drones. Using embedded technology, such objects can communicate and interact over the internet, with each other, the user, the service provider and/or their environment, and they can be remotely monitored and controlled.

This Practice Note provides an introduction to IoT technology and considers the following issues:

- The technology behind the IoT
- Identifying the legal issues

- Application programming interfaces (APIs)
- Telecommunications and electrical equipment
- Intellectual property—overview
- Intellectual property rights ownership and licensing issues
- Competition law
- Consumer protection
- Liability and fault
- Compliance requirements
- The appropriate contracting model
- Legal issues of the future

This Practice Note does not consider data protection, privacy or cybersecurity. These issues are addressed separately in Practice Note: Internet of things (IoT)—data protection, privacy and security.

The technology behind the IoT

The introduction of internet protocol version 6 (see: LNB News 27/05/2008 64), the availability of cheaper electronic technology, the ubiquity of connectivity (access to the internet, particularly via mobile phone networks) and cloud computing are some of the developments that have enabled rapid growth in the IoT.

Current applications of the IoT exist in:

- the health sector—particularly monitoring patients through wearable technology and

smart objects, known as e-Health

- agriculture—with ‘smart farming’ and the use of drones and autonomous and connected farm vehicles to increase efficiencies and yields
- advertising—using data collected through the IoT to provide targeted advertising services
- efficient living—the application of smart meters in the home to track and regulate energy consumption, smart home devices enabling remote control and smart speakers and personal assistants
- transport—connected vehicles capable of logging and transmitting vehicle, performance and driver data and facilitating autonomous functionality
- industry—enabling automated warehouses, manufacturing processes and automated delivery options
- public sector—enabling smart monitoring of public spaces and automated response across a variety of applications, ranging from police and public order to monitoring and maintenance of roads and public buildings and infrastructure

Growth areas and emerging applications for IoT technology include:

- smart cities—autonomous and remote management of maintenance and development through collected data; increased automation of facilities; use of video camera surveillance and facial recognition technologies
- increasingly intelligent and fully automated systems—as developments in artificial intelligence (AI) and M2M learning advance, their use in combination with the IoT will lead to increased capabilities for everyday objects and systems
- advances in security software—a likely focal point being the increased security of router technology—the entry point of the internet into the home
- autonomous and connected vehicles—continued development and growth in this sector is expected at pace

Industry 4.0

The rise of the IoT is linked to the coming about of Industry 4.0, a ‘buzzword’ used to describe the so-called ‘fourth’ revolution happening in manufacturing.

It began in the ‘third’ manufacturing revolution with the adoption of computers and automation and is said to be continuing through enhancements afforded by smart and autonomous systems; enabled by data and machine learning. The ‘smart’ factory is made possible through automation and machine intelligence.

A network of smart machines, digitally connected to one another and creating and sharing data, delivers efficiencies:

- identifying opportunities for optimisation quickly and efficiently using data analytics and the identification of patterns and insights, informing maintenance, performance and other issues
- utilising organic logistics and supply chains which automatically adjust to accommodate changes in input data, for example, adjusting manufacturing priorities to accommodate supply delays caused by weather
- driving autonomous vehicles, equipment and robotics

Identifying the legal issues

The application of the IoT, and its related technologies, continues to evolve, enabling new and innovative business models. The trend promotes a shift away from businesses and business models based on one-time product sales and towards models which deliver products which depend on, or are designed with, ‘value added’ services, delivered on an ongoing basis through software and the internet.

In 2015, Oliver Wyman identified six service patterns, accelerated by the IoT:

References:

The Internet of Things—Disrupting Traditional Business Models, Oliver Wyman, 2015

- reinforced product value—offering added value to an existing product, for example, adding sensors to sports equipment to allow players to analyse their game and improve their technique
- product to service—for example, predictive maintenance services offering services which complement the traditional physical product
- new service—available as a result of increased connectivity and available data
- service with no object—services facilitated by or arising out of other developments in the IoT
- product and service as a service—the ability to pay for products according to usage as a result of easy access to usage data facilitated by the IoT
- infinitely personalisable services—the IoT enabling services based on action and reaction pairs

Service models and patterns continue to emerge through innovative application and are combined with and applied to all types of product or service within any number of differing industry sectors.

This Practice Note draws out the key legal issues likely to be relevant to most IoT applications in the majority of circumstances, but in each case it will be important to carry out thorough due diligence, considering all aspects of the IoT application in all applicable jurisdictions to identify all relevant legislation.

New patterns of business and the contract structures underpinning them require careful thought in their design and formation, particularly in sectors like healthcare and financial services where there are likely to be additional layers of detailed specific regulatory rules to comply with.

This Practice Note does not consider legal issues arising in connection with:

- data—predicated on sensors and the collection and transfer of data, associated legal issues are high on the agenda in relation to the IoT. Companies that previously collected little or no information about their customers and products find themselves able to gather both product performance or usage data as well as personal customer data. Data protection and security compliance issues present a steep learning curve in such cases

- security—in addition to the existing body of law, regulators are increasingly focused on security, privacy and ethical concerns surrounding the application and development of this area of technology and are developing guidance, standards and regulations to address them. Building trust among consumers around the new infrastructures and capabilities is critical, particularly when set against the increasing consumer awareness of weaknesses and fallibilities of IoT devices and their susceptibility to hacks and data leaks

These issues are examined separately in Practice Note: Internet of things (IoT)—data protection, privacy and security.

Application programming interfaces (APIs)

The IoT relies on the interaction of devices and systems to achieve a defined task or goal. As such, communication between those devices and systems is key. Application programming interfaces (APIs) are a large part of enabling that communication.

An API is the ‘handshake’ associated with a particular piece of software that lets that other software connect to and communicate with it. It is a set of rules or policies that must be complied with to allow data to be exchanged and processed. A programmer can write a program based on one operating system which will work with or on different operating systems, without having to track through all of the details directly, provided that the API is in place.

The format of an API differs depending on the requirements of the application to which it enables connections. In its simplest form it may be just a document providing technical interface specifications for developers. At the other extreme, it may be an extensive set of software routines, protocols and tools to assist the development of applications

software routines, protocols and tools to assist the development of applications.

The treatment in law of APIs becomes increasingly important with the growth and development of the IoT as businesses try to use APIs to enhance their market position. In some circumstances, the developer of an API may be under an obligation to license that API, particularly where there are concerns around interoperability, as in the European Commission decision of *Case COMP/C-3/37.792—Microsoft*.

References:

Commission Decision of 24 May 2004 relating to a proceeding pursuant to Article 82 of the EC Treaty and Article 54 of the EEA Agreement against Microsoft Corporation, Case COMP/C-3/37.792—Microsoft

The legal requirements for interoperability and the related competition issues are considered in more detail below and in Practice Note: Internet of things (IoT)—data protection, privacy and security. The legal position on intellectual property rights (IPRs) is considered in the table below.

Information about APIs may be released to developers either:

- under licence, giving the owner greater control over the quality of software/apps developed by developers and the ability to generate revenue through charging a licence fee, or
- under an open model—the owner makes the API freely available so that software can be written for their platforms

or a combination of both.

For further information, see:

- Precedent: Application Programming Interface (API) licence agreement
- Precedent: API terms of use
- Application programming interfaces: API policy—checklist

- News Analysis: API licensing

Telecommunications and electrical equipment

Operators of IoT products and services must ensure that networks and devices comply with all relevant and applicable regulations and standards concerning telecommunications and electrical equipment.

In the EU, the provision of electronic communications networks and services in each Member State is governed by a common regulatory framework, which originally comprised five directives:

- Directive 2002/21/EC of the European Parliament and of the Council of 7 March 2002 on a common regulatory framework for electronic communications networks and services as amended by Directive 2009/140/EC (EU Framework Directive)—see Practice Note: Electronic communications: Framework Directive [Archived]

- Directive 2002/20/EC of the European Parliament and of the Council of 7 March 2002 on the authorisation of electronic communications networks and services as amended by Directive 2009/140/EC (EU Authorisation Directive)—see Practice Note: Electronic communications: Authorisation Directive [Archived]

- Directive 2002/19/EC of the European Parliament and of the Council of 7 March 2002 on access to, and interconnection of, electronic communications networks and associated facilities as amended by Directive 2009/140/EC (EU Access Directive)—see Practice Note: Electronic communications: Access Directive [Archived]

- Directive 2002/22/EC of the European Parliament and of the Council of 7 March 2002 on universal service and users' rights relating to electronic communications networks and services as amended by Directive 2009/136/EC (EU Universal Service Directive)—see Practice Note: Electronic communications: Universal Service Directive [Archived]

- Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the

electronic communications sector as amended by Directive 2006/24/EC and

Directive 2009/136/EC (EU ePrivacy Directive)—see Practice Note: EU regulatory framework for electronic communications—ePrivacy Directive

The objective of these directives was to establish a harmonised framework for the regulation of electronic communications networks and services throughout the EU. In December 2018, Directive (EU) 2018/1972 establishing the European Electronic Communications Code (Recast) (the EU European Electronic Communications Code (EU EECC)) came into force. The EU EECC consolidates four of the directives (excluding the EU ePrivacy Directive) which make up the framework. For more on the implementation of the EU EECC in the UK and the EU, see Practice Note: The European Electronic Communications Code.

The EU EECC increases the scope of the regulatory framework by expanding the definition of electronic communications services (ECSs) to encompass both ‘number-based’ and ‘number-independent’ interpersonal communications services (NI-ICSs). This includes M2M communications and internet access services and, in principle, captures a range of devices (such as ‘smart speakers’ like Amazon’s Alexa and some types of internet-enabled TVs and other appliances) as ‘customer equipment’.

References:

Article 2(1), (4) *of Directive (EU) 2018/1972*

NI-ICS providers face a more limited set of obligations than traditional telecommunications providers, recognising the differences in delivery and control of these newer forms of communication compared to the more traditional communication service models. However, as technologies mature, and consumer behaviour evolves, it is likely that the rules on mass-market forms of communication will converge. The EU EECC provides that, for Europe, the Body of European Regulators for Electronic Communication should conduct regular review of the approach in order to ensure that the regulation keeps pace with the technology.

The UK implementation of the EU EECC does not revise the definition of ECSs in line with the definition in the EU EECC. In the UK, the definition includes internet access services, number-based NI-ICSs and any other services involving the conveyance of signals (including M2M services which allow for the automated transfer of data and information between devices with limited or no human interaction).

The definition of ECS does not include NI-ICS and instead certain provisions are applied specifically to the category of NI-ICS.

The amendment of the definition of ECS in this way has wider implications for other legislation that relies on the definition. For example, the Privacy and Electronic Communications (EC Directive) Regulations 2003 (PECR 2003), SI 2003/2426 refer out to the ECS definition in the Communications Act 2003. Unless PECR 2003 are amended to expressly include NI-ICS, such services will not fall within their scope.

Intellectual property—overview

The technologies involved in an IoT product or service may include sensors and actuators, wired and wireless networks, computing and storage, analytics, user interfaces, algorithms and databases.

The underlying IPRs and related considerations are likely to differ depending on the maturity of the technology. The IoT is based around the concept of ‘improving’ existing technologies or giving them new or ‘smarter’ applications. In such cases, the relevant IPRs will include older, established portfolios and features that have already been licensed or monetised, each being applied in new or unprotected fields.

Established suppliers and new entrants will, in equal measure, need to review portfolios and ensure that they have sufficient licences in place to allow them to operate freely and take appropriate action to ensure the protection of any new intellectual property that may arise, that they create, or that is created on their behalf.

Intellectual property is important in the IoT both in terms of protecting and enforcing proprietary rights and avoiding infringement. The prevalence of technical standards (for example, technology standards such as 4G and 5G) complicates the landscape as their licensed use is typically granted subject to specific restrictions which must be taken into account.

Smart IPRs

In addition to the IPRs that may arise in relation to the design or functionality of the IoTs device itself, further rights may arise by virtue of the fact that the device is ‘smart’ or is being used in a manner which connects it to the IoTs, as set out in the table below:

Data	In order to operate in a connected manner a device will collect data and share it. In the UK there is no concept of ‘ownership of data’ as such. However, ownership rights can accrue in relation to the recorded, aggregated or collected form of data.	Copyright in the specific instances of data. For more, see Practice Note: Copyright—protectable works. Database rights in the aggregated form of the data. For more, see Practice Note: Legal protection of databases in the UK.
Software and software formats	As the connected technology will interface and communicate with the internet, the relevant IoT system will include use of software applications. Computer programs may be eligible for copyright protection as ‘literary works’ under the Copyright, Designs and Patents Act 1988 (CDPA 1988).	For more information about the rights and their protection, see Practice Notes: IP rights in software and Copying software and copyright. For more information about licensing software, see Practice Note: Key issues in software licence agreements.
Graphical User Interfaces (GUIs)	GUIs may be patentable both in the UK and Europe. However, there are strict requirements that must be fulfilled in order for them not to be considered as merely presentation of information, which is excluded subject matter.	More information regarding the patentability of GUIs at the EPO can be found in the EPO Guidelines for Examination G-II, 3.7.1. More information regarding the patentability of GUIs at the UK Intellectual Property Office can be found in the Manual of Patent Practice, sections 1.40–1.47.
	GUIs can be registered as registered designs in Europe and the UK. This is likely to be a faster route to protection than patenting.	For more information about obtaining protection through a registered design, see Practice Notes: UK registered and unregistered designs and Community (EU) designs.
	Copyright may also exist in the GUI if the interface is ‘its author’s own creation’.	In Bezpecnostni softwarova asociace-Svaz softwarove ochrany v Ministerstvo kultury, Case C-393/09 (see digital health), the Court of Justice stated that ‘a GUI is not a form of expression of a computer program’ within the meaning of Article 1(2) of Directive 91/250/EEC of 14 May 1991 on the legal protection of computer programs and cannot be protected by copyright as a computer program under that directive. Nevertheless, such an interface can be protected as a work by Directive 2001/29/EC of the European Parliament and of the Council of 22 May 2001 on the harmonisation of certain aspects of copyright and related rights in the information

		society if that interface is its author's own creation. As a result of this division of copyright, it is prudent to ensure that contracts with third party software developers specifically state that ownership belongs to the commissioner for both copyright in the software and any separate copyright in the GUI.
APIs	The EU Software Directive (Directive 2009/24/EC), which was implemented into UK law by amendments to CDPA 1988 while the UK was a member of the EU, states that ideas and principles underlying any element of a computer program, including those underlying its interfaces, are not protected by copyright. Those rules remain valid under UK law. In *SAS Institute, Inc v World Programming Limited*, although not specifically in issue, the Court of Justice of the European Union stated that 'neither the functionality of a computer program nor the programming language and the format of data files used in a computer program in order to exploit certain of its functions constitute a form of expression of that program'. The judgment has been taken to support the position that APIs are not protected by copyright because they are functional in nature. The dispute was later heard in North Carolina, in the US, where the courts took a contrasting view, finding in favour of SAS. In the US, in a long-running case between Oracle America, Inc and Google, Inc, APIs ('declaring code and the structure, sequence and organization of the API packages') were assumed by the Supreme Court to be copyrightable and the copying of the API 'where Google reimplemented a user interface, taking only what was needed to allow users to put their accrued talents to work in a new and transformative program' was fair use and as such did not give rise to copyright infringement liability. However, this judgment did not set out a position on API 'copyrightability' and limited its findings to the circumstances of the case. As such the position remains unclear albeit that the US courts have to date taken an approach that is more protective of intellectual property. For more, see News Analysis: API licensing.	For more, see Practice Note: Copying software and copyright.
Patent	IoT systems involve multiple devices working together to achieve the output, leading to a variety of possible patenting scenarios, including: —patents covering all or parts of the device itself —patents covering the way that the IoT communicates with other devices —patents covering the software-implemented processes performed by the device or by another element of the system communicating with the device	For more information on patenting in general, see Practice Notes: Patents and excluded subject matter and Patent term, renewal and restoration and for information about patenting software, business methods and mathematical methodology, see Practice Notes: US, EPO and UK approaches to patenting software, US, EPO and UK approaches to patenting business methods and News Analysis: Patenting AI in

		Canada, the UK and Europe.
Copyright and designs	Copyright and/or design rights may arise in relation to new technologies developed around or in relation to a device or application in the IoT, including: —stylised logos —get-up —graphic symbols —marketing text (related to an IoT service or product) —software (see above)	CDPA 1988, Pt IV and Sch 4 and the Registered Designs Act 1949. For more information about designs and copyright, see Practice Notes: Protection and management of designs—a practical guide and Copyright—subsistence and qualification.
Trade marks / passing off	Logos / trade names / product names connected with the device or process	Sections 1 and 2 of the Trade Marks Act 1994. See Practice Notes: Trade mark registration—strategy and Introduction to passing off.

Intellectual property ownership and licensing issues

As the IoT is based around the interaction and interoperation of numerous devices and systems it often involves multiple parties and extends across multiple jurisdictions. This can lead to complications around joint or multiple ownership of intellectual property (see Practice Note: Joint ownership of intellectual property rights), and around the appropriate jurisdiction and governing law (see Practice Note: Getting the Deal Through: e-Commerce 2021).

The concept of applying new use cases to existing traditional technologies sits at the heart of the IoT, increasing the potential utility of a device for the end-user, but also increasing the risk of disputes as a new wave of potential applications or claims are made available to underlying patent holders.

This convergence of technologies leads to an increase in licensing opportunities for standard essential patents (SEPs) holders, as more companies begin to make use of standardised wireless connectivity technology (see below for more on SEPs). Entities that have not traditionally been competitors, or otherwise had significant interactions, may find themselves encroaching on each other’s technological spaces through the emergence of the IoT.

Existing patent portfolios, when applied among newly aligned competitors is likely to lead to increased litigation and a disparity in licensing leverage. Traditionally a patent portfolio is

built for the dual purpose of offensive patent assertion and defensive patent protection—with extensive cross-licensing practices between competitors where mutually beneficial.

However, this strategic equilibrium is knocked out of balance by the IoT as companies are exposed to a completely new set of competitors against which they do not have defensive patents to assert. This creates an imbalance in negotiating power, removing the opportunity for cross-licensing and increasing the likelihood of litigation.

As an emerging growth sector, the IoT is also prone to unwelcome attentions of 'Non-Practicing Entities' or 'Patent Trolls'. Third parties that buy up patent portfolios with the sole intention of litigating them against new technologies.

All parties in an IoT process or system may be susceptible to a claim being brought against them, regardless of their respective size or commercial input and the threat of such litigation poses a particularly big risk for start-ups, that lack the resources to engage in prolonged legal battles.

Patent pools

The IoT is leading to the proliferation of new patent pools, with a view to mitigating the increased litigation risks identified above. A patent pool is an agreement between several patent owners to license their patents to each other or to third parties, thus removing litigation risk and promoting innovation and collaboration between the members. For example, a pool may allow implementers to obtain a licence to all (or a substantial part) of the relevant patents required to practice a certain technology without the need to negotiate royalties with each patent holder individually.

Examples of established patent pools include:

- Avanci, a pool for essential wireless patents backed by Ericsson, Qualcomm, Interdigital, Sony, ZTE and others. Avanci licences are made available at a flat rate where a fixed amount is paid for each unit produced or sold
- MPEG-2, MP3 and DAB

It is possible for patent pools to be considered restrictive of competition, as they necessarily

involve the joint selling of the pooled technology. In the EU, however, the extended provisions of the latest version of the Commission's Technology Transfer Block Exemption

(TTBE) Guidelines clarify the application of the safe harbour to technology pools. Patent pools generally fall outside of the scope of the prohibition in Article 101(1) as long as certain conditions are met, including that only essential technologies are pooled, and that these are licensed out on fair, reasonable and non-discriminatory (FRAND) terms. For more information on patent pools, see Practice Note: EU Competition law and intellectual property. See also Practice Notes: The effect of Brexit on UK competition law.

Standard essential patents (SEPs)

Systems which incorporate by design the concept of connectivity are usually subject to technical standards or specifications that identify certain features of a class of products or procedures. The primary objective of many technical standards is to allow interoperability between components or products manufactured by different entities. The standard defines technical 'rules' which allow, for example, communication between devices. The administrative framework provided for by the wider standardisation process enables rapid development and deployment of the technology in question with high degrees of interoperability between products.

Where the subject matter of a patent overlaps with functionality that features in a technical standard such that the patent would inevitably be infringed by operating in accordance with the technical standard, that patent may be considered a SEP. Often SEPs carry with them an obligation to grant licences to those who wish to practise the relevant standard. The precise nature of the licensing obligations imposed on the SEP will depend on the standard setting organisation involved, for example, the European Telecommunications Standardisation Institute (ETSI) IPR policy requires SEP holders to give an undertaking to license their SEPs on FRAND terms if they wish to participate in standard setting.

Agreeing the correct FRAND rate is further complicated by the convergence and novel application of technologies as rates set and deemed appropriate when applied in one sector may be argued to become absurd or discriminatory when applied in another, with varied and wide-ranging price points and products.

For more detailed information about SEPs and related disputes, see Practice Note: Standard essential patents and FRAND licensing. For a consideration of the competition issues arising

in relation to SEPs, see below.

Competition law

The IoT, and the related shifts in markets and business models, has received attention from competition law and related regulators. The potential for dominance among traditional and new participants and via new delivery models has led to a growing role for competition law in this sphere.

At a policy level, issues of roaming, interoperability, portability and ease of switching between platforms, applications and devices are becoming more prevalent and maintaining competition within, or in spite of, the IoT increasingly relevant.

Technology Transfer Block Exemption

In the EU, Article 101 of the Treaty on the Functioning of the European Union (TFEU) prohibits agreements which prevent, restrict or distort competition within the EU internal market. Such anti-competitive agreements are illegal under Article 101(2) TFEU unless they fall within a block exemption or can be explicitly justified on efficiency grounds under Article 101(3) TFEU. One of the block exemptions providing a 'safe harbour' from breaching Article 101 is Regulation (EU) 316/2014, the EU Technology Transfer Block Exemption Regulation (EU TTBER) which covers technology licensing agreements in relation to most IPRs, including know-how.

On 1 January 2021, EU competition law ceased to apply in the UK. However, activities conducted by a UK business in the EU remain subject to EU competition law and any applicable domestic competition law of EU member states. The European Commission also continues to have jurisdiction over anti-competitive agreements that affect trade between EU member states, but it can no longer enforce Article 101 directly in the UK, ie it cannot request information or enter and search premises in the UK. Where an agreement affects trade in the UK, domestic competition law continues to apply. The UK domestic equivalent of the Article 101 TFEU is Chapter I of the Competition Act 1998. This provides for the so-called Chapter I prohibition in the UK.

Prior to 1 January 2021, EU block exemptions applied 'in parallel' under UK competition law meaning that agreements were exempt from the Chapter I prohibition if they were

covered by an EU block exemption. On 1 January, the TTBER was converted into domestic UK law. Retained Regulation (EU) 316/2014 (UK TTBER) provides 'retained exemptions' from Chapter I prohibitions. This means that agreements which benefitted from the parallel TTBER exemption prior to 1 January 2021 continue to benefit from a retained exemption in the UK.

For more information, see Practice Notes:

- EU competition law and research and development agreements
- Applying block exemptions to IP agreements
- Assessing IP-related agreements under the Technology Transfer Block Exemption Regulation
- Assessing IP-related agreements outside the Technology Transfer Block Exemption Regulation

Companies which have not previously manufactured or sold connected devices may need to seek to negotiate licences, for which the TTBE (and/or the UK TTBER) is likely to be relevant, as it offers a safe harbour for licences of technology rights (including patents) that meet the conditions set out in the Block Exemption. In negotiations, patent holders may also wish to consider whether they can limit the fields of use of any licences granted. Where licence negotiations are unsuccessful, an increase in litigation is likely. This is discussed in more detail below in the context of SEPs. It is arguable that the TTBE does not provide a safe harbour for licences of SEPs, given the relatively low market share thresholds that must not be exceeded for the Block Exemption to apply, and the views often expressed that SEPs owners hold dominant positions. Of course, if the licence contains no restrictions of competition, then no exemption is necessary.

Where a licensee improves the licensed technology the licensor may wish to ensure it can share in the benefits of any such improvements through a 'grant back' obligation imposed upon the licensee. The licensing of rights in this way can create competition issues. Non-exclusive grant back obligations are also covered by the safe harbour of the TTBE.

However, exclusive grant back obligations, which prevent the licensee from exploiting the improvement either for its own production or by licensing out to third parties, are excluded from the TTBE and are subject to individual assessment. Exclusive grant backs may affect competition in innovation, although if the licensor pays consideration in return for the exclusive grant back it is less likely to create a disincentive for the licensee to innovate.

For more information, see: Competition, IP rights and Technology Transfer Block Exemption—overview and Practice Note: The effect of Brexit on UK competition law.

Big data

The IoT facilitates the collection of large volumes of data, which can be used for targeted marketing, smart pricing, demand estimation etc. As a result competition bodies are looking at the potential impact of this data collection on market power.

Digital data ecosystems have enabled some of the most profitable, valuable and powerful business models currently in existence, examples include Apple, Google, Facebook and Amazon. Data monopolies are a consideration for merger clearances and interesting questions arise around whether big data should form a separate market of its own for the interests of determining dominance. Another pertinent question is whether such data may amount to an ‘essential facility’ from which it would follow that, depending on the circumstances, unjustified refusal to grant access to data generated by IoT devices could amount to a breach of competition law.

Data portability is required under both the UK and EU General Data Protection Regulation regimes, granting data subjects the right to transmit their personal data to another controller. For more, see Practice Note: Internet of things (IoT)—data protection, privacy and security.

In the EU, the European Commission has outlined its vision for a ‘genuine single market for data’ in its communication on a European Strategy for Data. Two pieces of legislation have been proposed: the Data Governance Act and the Data Act.

References:

EC—a European Strategy for data

The Data Governance Act (or Regulation on European data governance) establishes a framework to facilitate general and sector-specific data-sharing while the Data Act aims to

clarity, for EU consumers and businesses, the use and access to data in business-to-business

and business-to-government situations. See: LNB News 01/12/2021 19 and News Analysis: EU's draft Data Act aims to 'unlock' industrial data for new services.

References:

Proposal for a Regulation on European data governance (Data Governance Act)

SEPs

Most SEP holders and implementers of SEPs manage to resolve licensing disputes by reaching commercial agreement without resorting to litigation. However, when negotiations do break down, SEP holders often allege that implementers attempt to ‘hold out’ from taking a licence by continually delaying negotiations, and implementers often claim that SEP holders are attempting to ‘hold up’ innovation by refusing to license implementers or by seeking unduly high royalties.

The Commission has drawn attention to the potentially abusive behaviours of holders of SEPs, for example (in cases involving Samsung in 2012 and Motorola in 2014) by confirming that it may be an abuse of dominance for a company to seek an injunction based upon an SEP against a company that is willing to take a FRAND licence. For more, see Practice Note: EU Competition law and intellectual property—Litigation by IP owners. The Court of Justice of the European Union has also set out a framework for licensing negotiations in *Huawei Technologies Co Ltd v v ZTE Corp* which includes practical steps for SEP holders and implementers to follow in order to avoid the risk of abusing a dominant position under Article 102 TFEU. For more, see News Analysis: Standard essential patents and injunctions in Huawei v ZTE—is the law patently clear?

References:

COMP/39.939—Samsung Electronics Enforcement of UMTS standard essential patents

Case AT.39985—Motorola-Enforcement of ETSI standard essential patents

Huawei Technologies Co Ltd v v ZTE Corp, Case C-170/13, [2015] All ER (D) 237 (Jul)

The Commission built upon the Court of Justice of the European Union’s decision, and other case law developing throughout EU Member States, in its 2017 Communication, ‘Setting out the EU approach to Standard Essential Patents’, which offers guidance on how *Huawei v ZTE* should be applied, and outlines a series of general FRAND licensing principles. In 2020, the Commission published a further Communication setting out an EU action plan for intellectual property more generally, which addresses potential future EU developments in

the SEP space. This was followed by a report by the Commission's independent Group of Experts on Licensing and Valuation of SEPs in 2021. In February 2022, the European Commission launched a call for evidence seeking views on its proposal to develop an improved framework for SEP licensing, aiming to make it more transparent and predictable. Evidence may be submitted until 9 May 2022.

References:

Communication from the Commission to the Institutions on Setting out the EU approach to Standard Essential Patents

Communication from the Commission on Making the most of the EU's innovative potential —An intellectual property action plan to support the EU's recovery and resilience

Contribution to the debate on SEPs: Group of Experts on Licensing and Valuation of Standard Essential Patents (E03600)

European Commission: Intellectual Property—new framework for standard-essential patents

In the joined appeals of *Unwired Planet v Huawei* and *Huawei v Conversant*, the UK Supreme Court was required to consider the *Huawei v ZTE* framework and, in doing so, confirmed that the only mandatory condition was the requirement for the SEP holder to notify or consult with the alleged infringer before bringing a claim for an injunction. Compliance with the other steps in the *Huawei v ZTE* framework is not mandatory but does give the SEP holder 'safe harbour' against a finding of abuse of dominance, see News Analysis: Supreme Court—English courts can determine terms of global licences for portfolios of standard essential patents (Unwired Planet v Huawei).

References:

Unwired Planet International Ltd v Huawei Technologies (UK) Co Ltd; Huawei Technologies Co Ltd v Conversant Wireless Licensing SARL; ZTE Corporation v Conversant Wireless Licensing SARL [2020] UKSC 37

It is also possible for licence offers made by SEPs holders to raise issues of excessive pricing under Article 102(a) TFEU, or discrimination under Article 102(c) TFEU. A SEPs holder that insists on a licence that 'bundles' SEPs and non-SEPs may also risk abusing a dominant position (see first instance decision in *Unwired Planet International Ltd v Huawei Technologies Co Ltd* and New Analysis: In brief: High Court clarifies approach to determining FRAND royalties for Standard Essential Patents (Unwired Planet v Huawei Technologies)).

References:

Unwired Planet International Ltd v Huawei Technologies Co Ltd [2017] EWHC 1304 (Pat), *paras [785]–[791]*

As with any potential competition issue, the question of whether certain patents are essential

As with any potential competition issue, the question of whether certain patents are essential and whether an entity abuses its dominance or otherwise infringes competition law should

be addressed on a case-by-case basis and expert competition advice should be sought if thought relevant.

As smart technologies are likely to be based on a large number of patents across a wide ranging field of patent holders, issues of this nature are likely to be the subject of further litigation in the future.

For more information about the abuse of dominance and competition law in intellectual property, see Practice Notes: The prohibition on abuse of dominance, Competition law and intellectual property and IP Rights and abuse of dominance.

For more information about SEPs, see Practice Note: Standard essential patents and FRAND licensing.

Interoperability and standards

Another aspect of the IoT and competition law relates to standardisation and interoperability, as many IoT products are based on or around proprietary platforms and standards. Interoperability lies at the heart of the IoT: the ability of devices and systems to talk to each other using open shared protocols regardless of the type of content or where it is transferred from or to. However, in reality many industrial and home networks were not originally designed to be connected globally.

There is a degree of fragmentation of standards in the IoT and layering; with standards being produced by intergovernmental organisations (like ETSI, Institute of Electrical and Electronics Engineers or Internet Engineering Taskforce) and industry consortia formed around a common protocol. The development of diverging standards has the potential to prevent device interconnectivity, which may, for example, result in the products of certain manufacturers being ‘locked out’ of smart systems and consumers being ‘locked in’ to a product manufacturer for the maintenance and repair of products that they have bought or for a range of products related to a particular smart system.

It can be an abuse of a dominant position under Article 102 TFEU if a dominant company refuses to provide interoperability information and to allow its use for development purposes

(for example, in cases involving Microsoft's tying of its media player and browser to its

operating system). For more, see Practice Note: Tying and bundling—the challenge of new markets to Article 102 TFEU.

References:

Case COMP/37.792 Microsoft (prohibition decision)

There are, generally speaking, two types of platform; the proprietary platform that will only permit devices to connect where they have been certified by the manufacturer of the IoT system; and, the open source platform, to which any device is able to connect.

The use of a closed system can benefit competition by increasing inter-system competition, providing companies with an increased incentive to enter and to innovate in order to try and capture greater market share. They can also generate efficiencies such as ensuring compatibility between components, enabling user coordination and avoiding free-riding.

However, open systems are more likely to achieve the full benefits of network effects and economies of scale for component makers, as well as generating intra-system competition. Market entry through component innovation is also more likely.

Both open and closed systems raise the prospects of firms acquiring market power or even a monopoly, due to network effects and switching costs (which is particularly an issue in closed systems). A dominant or monopolist platform may be able to foreclose component suppliers, making it more difficult for other platforms to enter.

In addition to its 2004 decision against Microsoft regarding interoperability, the Commission fined Google €4.34bn in 2018 for its practices regarding its open Android mobile operating system, and has also recently investigated Amazon's Marketplace and Apple's App Store (in response to a complaint from Spotify). Interoperability has also been an issue in merger control. In the case *M.5669 Cisco/Tandberg*, the acquisition was approved conditional upon the divestment of a protocol developed by Cisco for its videoconference solutions, called 'TIP', to ensure the interoperability of the merged entity's products with those of its competitors.

ETSI is conducting a number of standardisation initiatives covering a wide range of the applicable technologies.

References:

ETSI—Internet of Things

In July 2020, the Commission launched an antitrust competition inquiry into the IoT and consumer-related products and services in the EU. The inquiry focused on networked products that can be controlled at a distance (via voice assist or a mobile device), including smart home appliances and wearable devices. It addressed issues such as standards and protocols governing the use of the products and services, how services are integrated within devices (downloaded or pre-installed), the nature and extent of interactions with virtual assistants, exclusivity arrangements, and the handling of personal data. The relevance of SEPs was also considered. For more, see: LNB News 16/07/2020 60.

In June 2021, the preliminary results of the inquiry were published identifying four main areas of concern, as follows:

- exclusivity and tying practices in relation to voice assistants, as well as practices limiting the possibility to use different voice assistants on the same smart device
- the position of voice assistants and smart device operating systems as intermediaries between users, on one side, and smart devices or consumer IoT services on the other side, combined with their key role in the generation and collection of data, allowing them to control user relationships
- providers of smart device operating systems and voice assistants extensive access to data, including information on user interactions with third party smart devices and consumer IoT services, giving them advantages in relation to the improvement and market position of their general-purpose voice assistants, and allowing them to leverage more easily into adjacent markets
- the prevalence of proprietary technology leading at times to the creation of ‘de facto standards’, together with technology fragmentation and lack of common standards, raising concerns as to the lack of interoperability in the consumer IoT sector

For more, see: LNB News 09/06/2021 82.

The final report was published on 20 January 2022, identifying potential competition concerns in the growing markets for IoT related products and services in the EU and

confirming concerns identified in the preliminary report (as outlined above). The results of the inquiry will provide guidance to the Commission's future enforcement and regulatory activity and will inform its implementation of its digital strategy and the proposal for the EU Digital Markets Act. For more information on the EU Digital Markets Act, see Practice Notes: EU Digital Markets Act—progress tracker and The EU's Digital Markets Act.

References:

EC: Final report—sector inquiry into consumer Internet of Things

Maintenance and repair

As IoT business models emerge combining the sale of the product with an ongoing lifetime operation and maintenance service model (to be provided by the manufacturer) there is a risk that consumers find themselves 'locked in' to the product manufacturer for these operational and maintenance services, raising issues under the Enterprise Act 2002 and abuse of dominant position (under section 18 of the Competition Act 1998).

Consumer protection

General consumer protection legislation will still apply with regard to the IoT. Some of the more pertinent pieces of legislation are considered below. For a summary of the key consumer protection legislation, see Practice Note: Key consumer legislation—summary.

The European Commission identified a need to address consumer trust in the uptake of emerging digital technologies, and notably those technologies related to the IoT. A key factor is the requirement for a legal framework to provide remedies to injured parties. The current liability framework is considered to be adequate to deal with most liability issues but there is a recognition of the need to reflect on future needs and developments, to provide legal certainty to both businesses and consumers.

In October 2021, the European Consumer Organisation (BEUC) published a position paper on the subject of protecting European consumers in the world of connected devices. The paper outlined a series of recommendations on various areas, including cybersecurity, data protection, contractual rights, product safety and durability, and competition.

References:

BEUC: Protecting European Consumers in the World of Connected Devices—Position

Paper

Consumer Rights Act 2015

The Consumer Rights Act 2015 (CRA 2015) covers consumer rights and remedies for the sale of goods and the supply of services and digital content.

These rights and remedies apply to the IoT as much as any other type of consumer product. Where goods supplied include digital content, that digital content must meet the standards set out in CRA 2015 (ie it must be of satisfactory quality, fit for purpose and as described). If it does not comply with these standards, content will be treated as not conforming to the contract. The consumer will have a short-term right to reject and access to the tiered remedies available for non-conforming goods.

Any terms and conditions (including both contracts and notices) are subject to the unfair terms provisions of CRA 2015. Any terms must be fair and transparent. The transparency requirements can prove particularly challenging where complex technology and/or data flows are involved.

For detailed consideration of the application of CRA 2015, see Practice Notes:

- Consumer Rights Act 2015—summary
- Consumer Rights Act 2015—goods
- Consumer Rights Act 2015—services
- Consumer Rights Act 2015—digital content
- Consumer Rights Act 2015—unfair terms

Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013

In the majority of cases involving consumer contracts, there are requirements for the provision of information to the consumer, both prior to and after the formation of a contract, under the Consumer Contracts (Information, Cancellation and Additional Charges)

Regulations 2013 (CCR 2013), SI 2013/3134.

The specific requirements will vary depending on the sales model deployed specific to any particular instance within the IoT. In some cases, the consumer may enter into a contract on-premises or face to face, but it is probably more likely that the contract will be concluded at a distance (over the internet). For example, there are additional requirements in respect of distance contracts concluded by electronic means, regarding the information that must be provided immediately before a consumer places an order that places the consumer under an obligation to pay.

For a detailed checklist of the information requirements under CCR 2013, see: Information requirements under the Consumer Contracts (Information, Cancellation and Additional Charges) Regulations 2013—checklist. See also: Key consumer information requirements—checklist.

The provision of such pre-contract information to the consumer may prove challenging, depending on the technical constraints around the user interface, the likely customer engagement and the data and process flows behind the contracting/business model. There has been work at both an EU and UK level to create guidance on how best to provide information to consumers, while meeting the challenges of the digital environment. For more, see Practice Notes: Distance, doorstep and on-premises sales—Guidance on how to provide information to consumers and Consumer Rights Act 2015—unfair terms—Transparency test.

In January 2019, a ruling of the regional court in Munich that Amazon's 'Dash buttons' were in breach of German consumer law, on the basis that the button was not labelled with 'pay now' and other pre-contract information was not provided to consumers when purchasing with such buttons, was upheld. The 'Dash button' devices, which featured brand names and/or logos but no other wording, allowed consumers to place orders via Amazon by pressing the button on the device, without needing to confirm the order. Although the German legislation, implementing the requirement of Article 8(2) of the Consumer Rights Directive, is arguably drafted more narrowly than the equivalent requirement in CCR 2013 set out above, a failure to include any wording on such order buttons in the UK is also likely to breach CCR 2013. The judgment (in German) can be accessed here.

References:

BBC News: Amazon stops selling Dash buttons, 1 March 2019

BBC News: Amazon stops selling Dash buttons, 1 March 2019

Consumers entering into distance or off-premises contracts with traders also generally benefit from a 14-day cancellation right under CCR 2013. For more information on CCR 2013 generally, see Practice Note: Distance, doorstep and on-premises sales.

Product legislation

In 2008, the EU adopted a new legislative framework to 'improve the internal market for goods and strengthen the conditions for placing a wide range of products on the EU market'. The new framework came fully into force in 2017, placing responsibility for compliance at all levels of the supply chain, from designers and suppliers through to manufacturers, importers and distributors.

References:

European Commission: Single Market for Goods—New legislative framework

The legislation aims to improve market surveillance and the quality of conformity assessments and to clarify the rules around the use of CE marking, and is set out in the following:

EU legislation	Description	UK implementation
EU Radio Equipment Directive, Directive 2014/53/EU (EU RED)	Applies to all products which use the radio spectrum and defines essential requirements for health and safety, electromagnetic compatibility and efficient use of the radio spectrum. The EU RED applies to equipment using the radio spectrum which are placed on the European market. Importantly it does not apply to the 'relevant components' of radio equipment. The EU RED includes requirements for conformity assessments (that include safety and risks, including in relation to misuse), certification, and documentation (including traceability, numbering instructions and safety and technical documentation). The European Commission has published guidance on the EU RED. See: European Commission—Radio Equipment Directive (RED).	The EU RED is implemented in the UK by the Radio Equipment Regulations 2017, SI 2017/1206. The Office for Product Safety & Standards (OPSS) has produced guidance on the regulations. See: Office for Product Safety & Standards—Radio Equipment Regulations 2017—Guidance.

EU legislation	Description	UK implementation
EU Low Voltage Directive, Directive 2014/35/EU (EU LVD)	Applies to electrical products with an internal AC current of 50–1000V (which would include some smart IoT devices that do not use the radio spectrum but excludes smaller low voltage devices). The EU LVD includes requirements for market surveillance, conformity, and standards, similar to EU RED. The European Commission has published guidance on the EU LVD. See: European Commission—Low Voltage Directive (LVD).	The EU LVD was implemented in the UK by the Electrical Equipment (Safety) Regulations 2006, SI 2016/1101. The OPSS has produced guidance on the regulations. See: Office for Product Safety & Standards—Electrical Equipment (Safety) Regulations 2016—Guidance.
EU Electromagnetic Compatibility Directive, Directive 2014/30/EU (EU EMCD)	Works with the EU LVD, regulating interference with other equipment and the stability of electrical systems as opposed to safety (covered under the EU LVD). The European Commission has published guidance on the EU EMCD. See: European Commission—Electromagnetic Compatibility Directive (EMCD).	The EU EMCD was implemented in the UK by the Electromagnetic Compatibility Regulations 2016, SI 2016/1091. The OPSS has produced guidance on the regulations. See: Office for Product Safety & Standards—Electromagnetic Compatibility Regulations 2016—Guidance.
EU General Product Safety Directive, Directive 2001/95/EC	Applies to any consumer products (with a voltage below 50V (AC) or 75V (DC)) which are not subject to specific legislation. The market surveillance requirements are similar to the requirements under the other directives above but there are no CE marking or conformity requirements. Product safety is dealt with thorough self-certification and standards. Smaller, low-voltage IoT devices may fall within the scope of this directive. See also Practice Note: The EU General Product Safety Directive 2001/95/EC. Note that the European Commission published a proposal for a new General Product Safety Regulation on 30 June 2021. This proposal is part of the New Consumer Agenda. See Practice Note: EU General Product Safety Regulation—tracker.	The General Product Safety Directive was implemented in the UK by the General Product Safety Regulations 2005, SI 2005/1803. The OPSS has produced guidance on the regulations. See: Office for Product Safety & Standards—General Product Safety Regulations 2005—Guidance. See also Practice Note: General Product Safety Regulations 2005.

The framework includes other sector or industry-specific directives which may be relevant depending on the specific nature of the IoT system and related devices, such as the EU Toy Safety Directive, Directive 2009/48/EU (implemented in the UK by the Toys (Safety) Regulations 2011, SI 2011/1881).

The UK implementing regulations have been amended by the Product Safety and Metrology etc (Amendment etc) (EU Exit) Regulations 2019, SI 2019/696 (as subsequently amended by the Product Safety and Metrology etc (Amendment to Extent and Meaning of Market) (EU Exit) Regulations 2020, SI 2020/676), to address deficiencies arising from the UK leaving the EU and to make specific provision for the Great Britain market (some of the provisions apply differently in Northern Ireland). The OPSS has produced guidance for the application of the regulations as they apply to equipment being supplied in or into Great Britain from 1 January 2021.

References:

Office for Product Safety & Standards—Guidance: UK product safety and metrology

The medical devices sector, a sector in which the IoT is highly prevalent, is governed by a regulatory regime which imposes obligations on manufacturers to ensure that devices (including in vitro medical devices) are safe and fit for their intended purpose. For more, see Practice Notes: An introduction to the regulation of medical devices—EU Directives regime and The regulation of medical devices in the UK.

Product liability

The Commission (in particular the Digital Single Market (DSM) strategy) has emphasised the importance of legal certainty for the rollout of the IoT.

In its communication in 2016 on ‘Advancing the Internet of Things in Europe’, it committed to assessing whether the current EU legal rules for product liability were fit for purpose in the context of the IoT.

References:

European Commission Staff Working Document—Advancing the Internet of Things in Europe

In May 2017, the DSM midterm review stated that the Commission would consider adapting the legal framework to take account of emerging digital technologies, particularly civil law liability and the ongoing evaluation of the EU Product Liability Directive (Directive 85/374/EEC), the EU General Product Safety Directive (Directive 2001/95/EC) and the EU Machinery Directive (Directive 2006/42/EC) (implemented in the UK by the Supply of Machinery (Safety) Regulations 2008, SI 2008/1597, as amended by the Product Safety and

Metrology etc (Amendment etc) (EU Exit) Regulations 2019, SI 2019/696 (and as subsequently amended by the Product Safety and Metrology etc (Amendment to Extent and Meaning of Market) (EU Exit) Regulation 2020, SI 2020/676)). Revision of the EU Product Liability Directive is considered further below and in Practice Note: Defective products—Reform. To follow the progress of the review and evaluation of the EU Product Liability Directive, and the EU General Product Safety Directive, see Practice Notes:

- EU consumer protection—tracker
- EU General Product Safety Regulation—tracker

The Consumer Protection Act 1987 (CPA 1987) (as amended by the Product Safety and Metrology etc (Amendment etc) (EU Exit) Regulations 2019, SI 2019/696 (and as subsequently amended by the Product Safety and Metrology etc (Amendment to Extent and Meaning of Market) (EU Exit) Regulation 2020, SI 2020/676)) implements the EU Product Liability Directive. It creates a form of 'strict liability' where a product is shown to be defective.

CPA 1987 defines a defective product as one where the 'safety of the product is not such as persons generally are entitled to expect.' The types of damage for which proceedings may be brought include personal injury, death and damage to personal property to the value of more than 275 pounds. There is no liability for damage to the defective product itself.

For more information on product liability generally, see Practice Note: Defective products.

A difficult area in relation to product liability and the IoT is customer expectation. CPA 1987 defines a defective product as one where the safety of the product is not such as persons generally are entitled to expect. However, in the IoT, customers may have unrealistic expectations in terms of what the technology is capable of.

In judging whether the safety of the product is 'such as persons generally are entitled to expect' the court is required to take all of the circumstances into account, but sets out certain specific relevant considerations, including:

References:

Consumer Protection Act 1987, s 3

- the manner in which, and purposes for which, the product has been marketed, its get-up, the use of any mark in relation to the product and any instructions for, or warnings with respect to, doing or refraining from doing anything with or in relation to the product

  References:

  CPA 1987, s 3(2)(a)

- what might reasonably be expected to be done with or in relation to the product

  References:

  CPA 1987, s 3(2)(b)

It goes on to state that 'nothing in this [section 3] shall require a defect to be inferred from the fact alone that the safety of a product which is supplied after that time is greater than the safety of the product in question'.

References:

CPA 1987, s 3(2)

It is important to note that CPA 1987 does not restrict consideration to the uses specified by the producer. So long as what is done can reasonably be expected, there can be liability. Therefore, there may be liability for some misuses of the product so long as these were foreseeable and not unreasonable. In an Austrian Supreme Court case in 1998, the court imposed liability on the producer of cycle handle bars because they had not warned they were unsuitable for racing conditions. Although not explicitly advertised for use in extreme conditions, the producer was held to be liable because it had been informed that top Austrian sportsmen were using their products in cycle races.

With more conventional products this would typically be achieved through an instruction manual delivered with the product packaging or warnings on the product or packaging itself. However, in the context of more intelligent and automated products, systems and services, in order to be meaningful and effective, warnings may be required at numerous points in the delivery model and may need to be more extensive. In some scenarios it may in fact be more appropriate to provide some form of user training to enable the consumer to use the product or service safely and in accordance with the manufacturer's intended design. The scope and sufficiency of the training would depend on the complexity and nature of the delivered

service or product.

In designing a ‘smart’ product or service the operator should consider, as good practice, the effective provision of relevant consumer warnings at multiple levels of the delivery model, including the operating manual, within terms and conditions for the use and upgrade of any related software or operating system, in user agreements related to the product or service and more regularly as reminders via the customer user interface.

Providing meaningful warnings and or advice may also prove a challenge depending on the user interface for the device or service in question. Some manufacturers have addressed this by linking to another device which offers greater functionality—such as a ‘smart’ phone.

For further guidance on the key issues for consideration by a business when designing systems to manage product liability risk, see: Product liability—product safety—checklist.

As with any claim under CPA 1987, defences are available and it may be possible to claim that the customer contributed to any damage in their negligent operation of the product or services.

It may also be possible to raise the state of the art defence, CPA 1987, s 4 (also known as the development risks defence). The defence requires that ‘the state of the scientific and technical knowledge was not such that a producer of products of the same description might be expected to have discovered the defect’. Particularly relevant in relation to cybersecurity, where the battle between the cyber attackers and the security technologies rages and is constantly advancing, and where it might be open to the manufacturer to argue that it would not have been possible to envisage the type of hack deployed prior to it having been so deployed.

References:

CPA 1987, s 4

To assist in this defence manufacturers would be advised to keep detailed records of their efforts to keep abreast of developments in relevant technologies and to document their state of knowledge during development processes.

This defence may also become particularly relevant in the context of AI and machine learning. Where machines might, in the future, be capable and encouraged to freely learn

from their context and adapt and change their delivered service accordingly (without human intervention) it would be open to the manufacturer to argue that the damage causing

outcome of the technology could not have been identified either before launch or even during operation. The availability of this defence is then, perhaps, questionable in terms of encouraging responsible action in placing of truly autonomous systems on the market.

For further guidance, see Practice Note: Defences to a claim under the Consumer Protection Act 1987.

Within the UK, in 2021, the OPSS published the outcome of its consultation of the UK product safety review, which considered whether the domestic product safety regime is fit for the future and in particular with regard to opportunities for product safety in respect of new products, digital technologies and new models of supply (see: LNB News 11/11/2021 63). Alongside short-term actions not requiring legislative change, the outcome made a commitment to putting forward proposals for consultation on legislative change around an 'ambitious and multi-faceted reform programme' for the regulation of product safety in the UK.

References:

Office for Product Safety & Standards—Guidance: UK product safety and metrology

Consumer protection at the EU level

EU legislation specifically expands the scope of current consumer directives to include 'smart goods'. There are also key developments concerning the regulation of digital content and digital services under various pieces of EU legislation; in particular:

- the 'New Deal for Consumers' package—made up of Directive (EU) 2019/2161, the EU Omnibus Directive and Directive (EU) 2020/1828, the EU Collective Redress Directive
- DSM strategy—made up of Directive (EU) 2019/770, the EU Digital Content Directive and Directive (EU) 2019/771, the EU Sale of Goods Directive

For more information, see Practice Notes:

- The EU Omnibus Directive

- The EU Digital Content Directive, and
- The EU Sale of Goods Directive

See also Practice Notes: EU consumer protection—tracker and Key EU consumer legislation—summary.

Liability and fault

The IoT works based on sensors and automation, with less and less consumer input. Where sensors or connectivity fails there may be new or additional liabilities for the manufacturers and maintenance providers of those sensors and networks as causation shifts from human operator to device failure. Additionally, as providers venture out of their traditional supply models into new sectors they are likely to be exposed to new and differing liability models, playing differing roles in the chain of causation and being exposed to new and increased liability risks.

As the IoT spreads its reach and becomes ever more intelligent and capable, there are more potential parties to a claim, the network provider, the data storage facility, the device manufacturer, the maintenance and support operator, the encryption provider, the payment methodology and so on.

In cases where IoT products or services cause damage it may be difficult to identify and allocate the responsibility for that damage, due to the breadth and variety of entities involved in the relevant instance of operation. Complexity arises due to the interdependency between the different components and layers of service and operation; the devices themselves; enabling software components and applications; enabling and transactional data; services relating to the data (its collection, processing, compiling, analysis), and the connectivity or network on which the IoT communicates. This interdependency gives rise to questions as to who should be held liable in the event that the technology causes a damage and how to identify the root cause of the problem.

Looking at the liability framework in which the IoT resides, it is important to examine issues

which may arise in relation to both contractual liability and non-contractual liability (the violation of a right protected by law). Operators within the IoT sector will need to comply with both.

For more detail, see Practice Note: Consumer protection for defective or dangerous products—legal bases.

In terms of contractual liability, allocation of liability for an IoT product or service is most likely to be set out across various agreements between the relevant entities and at different stages of the application.

The convergence of new technologies caused by the IoT means that entities may find themselves contracting in unfamiliar market places and industry sectors. As traditional technologies enter new marketplaces, they may encounter unfamiliar model contract templates or find themselves being asked to sign up to industry codes or standards about which they have little to no experience.

It will be important, in such circumstances, to carry out proper due diligence of the legal and industry landscape into which they are delving and, good practice, at least in the first few instances, to seek robust legal advice.

As a result of new and emerging business models made possible by the IoT, a business may also find that provision of their product or service opens them up to new and/or increased liabilities under their contracts. For example, a mobile network provider—traditionally responsible for the connectivity in handsets etc, when offering to provide its network as part of a connected traffic management system, may open itself up to new liabilities should a network outage lead to a serious road traffic accident. Equally the provider of software to that network operator that fails to deliver a timely fix or patch, leading to a network outage, may be the cause of and responsible for that liability (where previously the extent of liability would be damages in respect of loss of mobile phone usage).

Questions then arise as to the reasonableness of the scope and extent of the liability that a provider can or should be commercially justifiably held to under a contract. For more information about the general principles, see Practice Note: Exclusion and limitation of liability

liability?

It is important to consider that there are some liabilities that cannot be excluded under contract (for example liability for death or personal injury caused by negligence). Such liabilities may have been relatively remote in terms of risk for the provider under traditional models, but much more likely and worthy of note under IoT applications.

In addition to the allocation of responsibility in the event of damage, it is also important to ensure safety over the lifetime and support of the product or service, to prevent or reduce the potential for such damage.

Technologies associated or embedded within the IoT must meet all relevant and applicable health and safety requirements. The nature and scope of those requirements will depend on the type of product or service being delivered in each case. Due to the nature of the IoT a service may extend across a number of industry sectors (each with their own industry-specific regulation or health and safety standards or requirements), involving different key players, different jurisdictions, etc. It will be important to map the different elements of the product or service carefully, to identify all relevant legislation and regulation and to allocate responsibility for compliance, both in relation to the initial offering and over the lifetime and support of the product or service.

In February 2020, in its Report on the Safety and Liability Implications of Artificial Intelligence, the Internet of Things and Robotics, the Commission identified the potential gaps in the existing liability and safety frameworks for IoTs in Europe and suggested opportunities for adaptation or adjustment of key legislation to afford the same level of protection to victims of emerging digital technologies as is provided for more traditional technologies.

References:

Report from the Commission to the European Parliament, the Council and the European Economic and Social Committee on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, 19 February 2020

European Parliament resolution of 20 October 2020 with recommendations to the Commission on a civil liability regime for artificial intelligence

The report considered that Council Directive 85/374/EEC (the EU Product Liability Directive) is still relevant and should be used against producers of defective AI systems

where they fall within the definition of products. However, the directive should be revised to provide for products generated by digital technologies, in particular AI and the concepts of 'products', 'damage' and 'producer' should be clarified. It called for the directive to be transformed into a regulation, to strengthen the European liability framework in a move from harmonisation to standardisation.

In its October 2020 resolution, the European Parliament concluded that the EU Product Liability Directive is not sufficient. It found that the EU Product Liability Directive provides recourse and remedy for harm caused by a third party where there is a 'fault-based action'. However, additional liability rules are needed to address claims against the operator of an AI system (both the front-end operator and the back-end operator).

The resolution recommendations were for a risk-based regulatory structure. High-risk systems (listed exhaustively) would be subject to a strict liability regime and operators would be mandated to carry liability insurance cover. Those systems not listed would be subject to fault-based liability with a presumption of fault on the AI operator (the operator having to show that it has abided by its duty of care). Annexed to that resolution, the European Parliament put forward detailed legislative proposals on a civil liability regime for AI (published in the Official Journal on 6 October 2021).

On 30 June 2021, the European Commission published an inception impact assessment setting out objectives to modernise liability rules to take account of the characteristics and risks of new technologies, including AI-equipped products and services. The feedback period for the initiative closed on 28 July. The Commission ran a consultation between October 2021 and January 2022: Civil liability—adapting liability rules to the digital age and artificial intelligence.

References:

EC: Civil liability—adapting liability rules to the digital age and artificial intelligence—inception impact assessment

EC: Civil liability—adapting liability rules to the digital age and artificial intelligence—consultation

Draft regulations are expected in the third quarter of 2022. To follow the progress of the proposals, see Practice Note: EU consumer protection—tracker.

Compliance requirements

The rules that generally apply to the internet will apply to the IoT in the same way (the transfer of data over the internet being an essential element of the IoT).

For instance, the compliance requirements for businesses operating websites such as those concerning e-commerce, advertising and marketing, intellectual property, disclosure of information, accessibility, consumer protection, unfair practices, illegal or harmful content, data portability, geo-blocking and privacy, are all likely to extend to websites or applications connected to or associated with IoT devices.

For more on website compliance and examples of the types of legal issues that may extend to IoT in this regard, see Practice Note: Websites—compliance requirements.

The appropriate contracting model

The connectivity and services model associated with the IoT moves the provider away from a traditional sale and purchase model and towards more complex, internet service models. Depending on the nature of the IoT product and services the contract may have to provide for some kind of system or device installation, connectivity to other devices or applications, the provision of ongoing services, maintenance repair and upgrade post-purchase etc.

A full analysis of the end-to-end operational model should be conducted, considering all elements of the proposed business model throughout the life cycle of the product. The contract will need to take account of each of those elements. For example, in addition to the standard product warranties in a sale and purchase agreement, the contract will also likely have to deal with some form of commitment to the provision of service levels, as you would expect to see in an agreement for the provision of software.

The contract between the provider and the consumer will also need to include and flow down, as appropriate, any undertakings that the provider may have given to its subcontractors or other third parties engaged in the end-to-end operational model. In drafting and agreeing terms the provider should be mindful not to overcommit or commit something which conflicts with terms agreed with such other third parties to avoid the risk of being left unable to deliver.

Legal issues of the future

Net neutrality

This is the concept that governments and internet service providers are required to treat all data on the internet equally and without discrimination or preference. However, 5G will bring new challenges for application of this concept. It is expected that 5G will boost a massive expansion in the role of networked connections and the idea that service providers should treat all data being transmitted over their networks with equal priority seems less defensible where the services in question might involve, for example, a heart monitor transmission to a hospital compared to YouTube video download. One of the key features of 5G is the opportunity for ‘network slicing’, segmenting the single physical single network into multiple virtual ones in accordance with particular use cases. This could enable more efficient apportioning of network resources, but could also allow network providers to charge different rates for different network tiers and to offer varying quality of service between them. Something which goes against the principles of net neutrality.

For more, see Practice Note: Net neutrality.

Automation and the removal of consumer choice

Although currently in relatively early stages of development and adoption in the majority of IoT applications, the automation of machine to machine decision making in the IoT raises potential competition issues.

For example, if, in the instance of a ‘smart fridge’ capable of monitoring supply and automatically replenishing itself when it runs low, the fridge manufacturer contracts with one single supermarket supplier for this supply there will likely be significant market disruption and potential competition considerations.

Automated or smart contracts

As the capability of IoT devices increases, complemented by the incorporation of additional technologies such as AI, M2M learning and blockchain, the likely applications will more and more frequently operate without human intervention. In order to execute certain actions

and more frequently operate without human intervention. In order to execute certain actions,

such as a fridge automatically replacing the milk in a fridge, machines will be capable of entering into contracts with other machines.

Smart contracts are self-executing contracts written in computer code which automate contractual provisions between contracting parties in the event that certain defined conditions are met. The code, and the agreements contained in the code, exist across a blockchain network.

For more on smart legal contracts; how they work, the different types of smart legal contract, and their enforceability under traditional UK contracting principles, see Practice Note: Smart legal contracts.

Insurance industry policy, public data and ethics

The extent to which the state and/or motoring insurance or health insurance companies should monitor individual's movements and health is likely to become and increasingly pertinent issue. Patients with chronic conditions may welcome smart implants and devices and applications in their homes that provide real-time information about their health to, and automatically alert, their doctor. However, questions about ensuring affordable access to insurance and healthcare, who should use and re-use the data generated and questions about whether otherwise healthy individuals could or should be monitored, remain.