Legal 500
Country Comparative Guides 2024

United Kingdom
TMT

Contributor

Shoosmiths LLP

Joe Stephenson

Partner | joe.stephenson@shoosmiths.com

Paul Nightingale

Principal Associate | paul.nightingale@shoosmiths.com

This country-specific Q&A provides an overview of tmt laws and regulations applicable in United Kingdom.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

United Kingdom: TMT

1. Is there a single regulatory regime that governs software?

There is no single regulatory regime that governs software in the UK.

A number of laws and regulations across various sectors are, however, relevant to software. These include general regulations covering consumer protection, advertising, employment, intellectual property and data protection, amongst others.

In certain limited circumstances, there are specific regulations for software, such as use of software in medical devices, and those around harm caused by software and computer systems.

2. How are proprietary rights in software and associated materials protected?

In the UK, the main form of protection for software is through copyright, which applies to the software code (whether source code or any compiled version), any algorithms, graphics, video and audio recordings, and any documents, specifications, user manuals and other materials associated with it. Copyright arises automatically in the UK on creation of an original work, and there is no need to register this. Copyright generally protects against copying – there is no protection against independent creation of similar software or materials, where actual copying is not reasonably evident.

The functional aspects of any software application are not generally protectable in the UK unless it can be shown that a software with similar functionality came about as a result of copying of any code, specification or design materials.

Software code "as such" is not patentable in the UK, but a software-related invention might be patentable depending on the context, i.e. where the contribution made by the software-related invention has a technical effect (such as where software is used to drive equipment, or improve performance of a computing system).

The "look and feel" of any software application may be protected by registered design in the UK, which can be a quick and cost-effective way to protect unique aspects of the user interface.

Software is often exploited in such a way that the source code and design materials are not disclosed to any licensee or user of the software. To the extent source code and design materials are kept confidential and reasonable steps have been taken to prevent disclosure to third parties, the laws of confidence and/or trade secrets will allow the software owner to protect and enforce their rights in that confidential information.

3. In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

In the UK, the first owner of copyright is the author or creator of the copyright works. Where a software developer, consultant or contractor creates software for a customer, then the software developer, consultant or contractor will own the copyright in the software code and any documents, specifications, graphics or other materials in the software.

The same is true for any invention or concept which may give software its technical effect. Rights to any invention will remain with the software developer, consultant or contractor, who will own the rights to the invention, and will be entitled to apply for patent protection.

If it is the intention that the customer owns all rights in software, it is, therefore, important to ensure that such rights, including in any inventions, concepts or ideas, and any software code, documentation or materials, are assigned to the customer under a written agreement which is signed by the software developer, consultant or contractor.

The position is made more complex where, for example, a software developer will use its own proprietary code, templates or specifications to build software for its customer for efficiency and to control costs. The software developer is unlikely to agree to assign its own proprietary materials to the customer, in which case, the customer should seek an assignment of any software and materials created specifically for it, together with a non-

exclusive, perpetual licence to use the software developer's own proprietary software and materials insofar as is necessary for the use and exploitation of the newly created software.

4. Are there any specific laws that govern the harm / liability caused by Software / computer systems?

Liability for harm caused by software and computer systems is governed predominantly by either contract law or the law of negligence. Where a business provides software to a consumer, chapter 3 of the Consumer Rights Act 2015 sets out various implied contractual terms that govern such supply of software, including that it is of satisfactory quality, fit for purpose and as described. Chapter 3 of the Consumer Rights Act 2015 also provides various remedies if those statutory rights are not adhered to.

5. To the extent not covered by (4) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

The Computer Misuse Act 1990 is the main legislation that criminalises unauthorised access to computer systems and data. The Computer Misuse Act 1990 criminalises access to computer systems and data which has not been authorised by the owner of the computer system.

6. Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a software vendor and customer, including any laws that govern the use of cloud technology?

Generally speaking, there are no technology-specific laws that govern the provision of software between a software vendor and customer in the UK, and no specific laws that govern the use of cloud technology.

However, where the customer is a regulated financial services firm (hereafter referred to as a "regulated firm"), certain rules and guidance may apply in these circumstances. Which rules and guidance apply in particular instances, and the extent to which they apply, will depend on factors such as: the vendor's role in practice, what the regulated firm's activities are, and the impact that the service may have on those regulated activities.

In general, the rules and guidance issued by the Financial Conduct Authority ("**FCA**") and the Prudential Regulation Authority ("**PRA**") are intended to be technology-neutral. As such, the rules and guidance are not "technology-specific", but apply in situations where the services provided are supported by technology, including cloud services.

Specific rules and guidance apply in two circumstances: (1) outsourcing, and (2) activities which may affect a regulated firm's operational resilience (i.e. the ability of a regulated firm and the financial sector as a whole to prevent, adapt, respond to, recover and learn from operational disruptions (these could include disruptions caused by the failure of technology on which the regulated firm depends)). In such circumstances, one or more of the following may be relevant:

1. The FCA's rules and guidance in chapter 8 of the Senior Management Arrangements, Systems and Controls handbook ("**SYSC**") within the FCA Handbook. SYSC 8.1 applies to outsourcing, meaning it can apply to SaaS. Depending on what activities the regulated firm carries out, SYSC 8 applies either as guidance or as rules.
2. The FCA's Finalised Guidance FG16/5 for firms outsourcing to the cloud and other third-party IT services.
3. The European Banking Authority ("**EBA**") Guidelines on Outsourcing Arrangements dated 25 February 2019 (EBA/GL/2019/02). The FCA and the PRA expect firms to continue to comply with the Guidelines, to the extent they remain relevant post-Brexit.
4. The PRA's Supervisory Statement of March 2021 (SS2/21) on Outsourcing and Third Party Risk Management. Although directed to PRA-regulated firms such as banks, building societies, PRA-designated investment firms, insurance and reinsurance firms, the PRA's drafting was reviewed by the FCA and the FCA's approach aligns with the PRA's. The Supervisory Statement is a useful tool in understanding how the EBA Guidelines are likely to be interpreted and applied by the UK regulators.
5. The FCA's rules and guidance relating to operational resilience, in SYSC. The main rules appear in SYSC 15A.
6. The PRA's rules and guidance relating to operational resilience, in the Operational Resilience sections of the PRA Rulebook. This is supplemented by PRA guidance in its Supervisory Statement of March 2022 (SS1/21) on Impact Tolerances for Important Business Services.
7. A shared policy summary on operational resilience, from the Bank of England, PRA and FCA, dated March

2021.

In some instances, a regulated firm may have to consider the impact of technology on its activities even where the provision of services does not amount to outsourcing, or is not considered relevant to the regulated firm's operational resilience. For example, the PRA's SS2/21 also discusses third party arrangements which do not involve outsourcing. Moreover, where a regulated firm is subject to the FCA's Consumer Duty, it will have to consider the impact of the services it receives from third parties on its ability to comply with the Consumer Principle and deliver good outcomes for retail customers.

In addition, sector-specific conduct rules may affect the services the regulated firm receives. For example, if a regulated mortgage lender uses a technology platform to support the provision of documentation to applicants and potential borrowers, it will have to ensure that the documentation produced complies with requirements set out in the Mortgages and Home Finance: Conduct of Business sourcebook. Similarly, a consumer credit lender who outsources tracing of debtors or debt recovery activity must take account of the rules on data accuracy and outsourced activities in the Consumer Credit sourcebook.

In short, where the service recipient is a regulated firm then, depending on the services and the impact of those services of the firm's activities, a complex and varied tapestry of rules and guidance could apply. Regulated firms should seek specialist guidance in this area, as there is no one-size-fits-all roadmap or solution for determining how to comply with the requirements.

Cloud service providers should be especially conscious of the extraterritorial effect of certain EU laws, including Regulation (EU) 2023/2854 (EU Data Act). The Act, which entered into force on 11 January 2024, contains provisions designed to avoid situations where customers become "locked in" to vendors' cloud services. From 12 September 2025, certain provisions become directly applicable that will require cloud service providers to support their customers in switching service providers in certain scenarios, and to reflect these terms into their customer contracts.

7. Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

Yes, it is typical for a software vendor to cap its maximum financial liability to a customer in a software transaction in the UK, although there may be certain areas of liability that are excluded from this cap (please see the response to Question 8 for further information on these excluded areas of liability).

There is no market standard level of cap in the UK, as a liability cap will depend on a range of factors unique to each transaction, including the respective negotiating positions of the customer and software vendor. That said, it is not unusual for the level of cap to range between 100% to 150% of the annualised or total value of the contract.

8. Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's liability to the customer or subject to a separate enhanced cap in a negotiated software transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

a. Confidentiality breaches – No typical position – deal specific. A customer will generally push for this area of liability to be excluded from any financial cap, whereas a software vendor will typically resist this position and will require confidentiality breaches to either be subject to the general cap on liability or to a separate enhanced cap.
b. Data protection breaches – Same as for confidentiality breaches (covered at (a)).
c. Data security breaches (including loss of data) – Same as for confidentiality breaches (covered at (a)).
d. IPR infringement claims – In the absence of unique deal-specific reasons that require a contrary position, this area of liability is typically excluded from any financial cap (usually linked to the IPR infringement indemnity).
e. Breaches of applicable law – Same as for confidentiality breaches (covered at (a)); although it is not uncommon for breaches, specifically of the Bribery Act 2010 and/or Modern Slavery Act 2015, by the software vendor to be excluded from any financial caps.
f. Regulatory fines – Same as for confidentiality breaches (covered at (a)).
g. Wilful or deliberate breaches – In the absence of unique deal-specific reasons that require a contrary position, this area of liability is typically excluded from

any financial cap. Please note, however, although there is English case law to aid interpretation, there is no single, settled legal definition of what constitutes a "wilful or deliberate breach", so the customer and software vendor may wish to consider including an agreed definition of these terms within the contract.

9. Is it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

It is not uncommon in the UK for source codes to be held in escrow for the benefit of the software licensee, particularly where the software is either bespoke (and the software licensor has retained ownership of IP in the software) or performs critical operations for the software licensee.

Escrow providers now offer escrow services for cloud-based software as well as for traditional "on premise" software. Options available for cloud may include access continuity for single-tenanted environments, where access credentials and documentation may be deposited in escrow, to allow the licensee continued access to the cloud environment in the event of a software vendor failure. Where the cloud environment is a "one to many" unrestricted cloud environment, the escrow provider may hold a separately hosted, mirrored instance of the cloud production environment (including source codes, deployment scripts and databases) to allow temporary continuity in the environment if the software vendor no longer supports the original service environment.

Commonly used escrow providers in the UK include Escrow London, Iron Mountain, LE&AS, NCC Group, and SES.

10. Are there any export controls that apply to software transactions?

The UK controls the export of software that is used in the military and where the software may be considered "dual use" where it can be adapted for military use. The UK Government website lists items that are restricted by category. Anyone looking to export restricted items will require an export licence. It is a criminal offence to breach the export regulations. Businesses looking to export less obvious "dual use" items (in particular) should, if unsure, check the Government's "consolidated list of strategic military and dual-use items that require export authorisation", available on the Government website (and which can change from time to time), or take legal advice on interpretation.

Separately, there are complex issues that arise when dealing with the export of software to certain countries, especially China and Russia, in respect of sanctions rather than export controls. It should be noted that sanctions can be applied against individuals, activities, states and organisations and can vary in nature from being asset freezes, to bans on dealing, to bans on providing financial support and banking facilities. Anyone looking to export to a country where there are sanctions in place should consult the relevant regulations for that jurisdiction. Several jurisdictions besides the UK (including the US and EU) have their own sanctions lists and export controls which may vary from those in the UK.

Many global businesses with trade or employees in certain jurisdictions (e.g. China) have 'Overseas IT Policies' which may restrict the taking and use of work and personal mobile devices, laptops, etc. when entering the country, so this should also be borne in mind when considering software transactions.

11. Other than as identified elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

There are no specific technology laws governing IT outsourcing in the UK.

12. Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

The Transfer of Undertakings (Protection of Employment) Regulations 2006 ("**TUPE**") provide the following significant protection for employees in an IT outsourcing situation:

- The primary purpose of TUPE is to automatically transfer the employment of individual staff from their current employer to a third party IT outsource provider on the same date that the service they perform is transferred to the third party IT outsourcing provider.
- The starting point under TUPE is that the individual employees transfer to the third party IT outsource provider on the same terms and conditions of employment (the name of their employer will change

and they will also join or have the option of joining the pension scheme offered by the third party IT provider).
- The transfer of employment takes place automatically by operation of law under TUPE and is not something that parties can choose to ignore.
- TUPE provides enhanced protection to employees in outsourcing situations as the dismissal of an employee with at least 2 years' continuous service where the sole or principal reason for the dismissal is the transfer itself is automatically unfair. The third party IT outsource provider must be able to show the dismissal was for an economic, technical or organisational reason that entailed a change in the workforce to avoid an automatic unfair dismissal finding, and even then, the dismissed employee can still challenge the fairness of their dismissal under general unfair dismissal law.
- The third party IT outsource provider is prevented from changing the terms and conditions of employees that transfer to it under TUPE if the sole or principal reason for the change is the transfer itself. Again, the third party IT outsource provider must be able to show that any changes to terms and conditions of employment are made for an economic, technical or organisational reason entailing changes in the workforce or the employment contract permits the change in question.
- TUPE requires the current employer to inform the employees about the proposed transfer and to consult with appropriate representatives of the employees if the third party IT outsource provider is proposing to take any measures/make changes to their employment terms after the transfer. The penalty for failing to comply with this obligation is a protective award of up to 13 weeks' uncapped pay to each affected employee.

13. Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

The primary legislation governing the UK telecommunications sector is the Communications Act 2003, as supplemented by the Wireless Telegraphy Act 2006.

The Communications Act 2003 established Ofcom as the independent regulatory body responsible for overseeing the telecommunications industry in the UK, and set out Ofcom's duties. Together with the Wireless Telegraphy Act 2006, the Communications Act 2003 provides Ofcom with powers within the UK, such as the right to grant licences to providers who wish to provide telecommunications services, and the enforcement of compliance with legislation and guidelines. Both Acts provide a regulatory framework which seeks to protect consumers, ensure there is fair competition, and uphold standards of content.

Further laws that supplement the governance of the telecommunications sector in the UK include:

1. The European Electronic Communications Code ("**EECC**"), which was transposed into UK law in late 2020. The EECC looks to improve service quality by making investment in infrastructures more attractive to companies, and to protect consumers by placing price limits on international calls, providing affordable services, and promoting better security;
2. The Telecommunications (Security) Act 2021, which seeks to enhance the security of telecommunications networks across the UK by requiring providers to have measures in place to identify and then reduce the risk of security breaches;
3. The Online Safety Act 2023 was given Royal Assent on 26 October 2023 and aims to protect the public online. The Act obliges technology companies to be more responsible for users' safety online including duties to implement processes and systems to reduce the overall risks that can occur. Additionally, the Act provides more control for users as to the content that users wish to see online and finding the best ways to report issues when they arise. Ofcom has been provided with extra enforcement powers such as the ability to fine companies up to £18 million or 10% of qualifying worldwide revenue (whichever is greater) and to take criminal action against senior managers who fail to ensure compliance;
4. The UK General Data Protection Regulation, which sets out how organisations must collect, store, and use individuals' data (see also Question 18); and
5. The Privacy and Electronic Communications Regulations, which protects individuals' privacy (see also Question 18).

14. What are the principal standard development organisations governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

To facilitate interoperability in a multi-vendor and multi-network environment but also across geographical

borders, the principal standard development organisations (**"SDOs"**) governing the development of technical standards are necessarily international, rather than specific to the UK.

For companies or individuals in the UK implementing wireless communication technologies or keen to participate in the development of the relevant standards, there are several key SDOs to consider:

- The European Telecommunications Standards Institute (**"ETSI"**) is recognised by the EU as a European Standards Organisation (**"ESO"**) but is global in its reach. ETSI supports the development, ratification and testing of standards for ICT-enabled systems, applications and services, including 4G and 5G mobile communications.
- The International Telecommunication Union (**"ITU"**) whose Telecommunication Standardization Sector (ITU-T) defines standards for ICT networks and devices including the Optical Transport Network and advanced broadband access technologies such as Fibre to the Home and G.fast. In collaboration with IEC and ISO, ITU is also responsible for developing standards for video coding, with video accounting for the vast majority of all Internet traffic.
- The Institute of Electrical and Electronics Engineers (**"IEEE"**) Standards Association develops global standards in a broad range of technologies including computer networking standards for both wired and wireless networks.

These SDOs are also developing new standards specifically for the Internet of Things (**"IoT"**), digital health and connected vehicles. For example, there is a working group within IEEE for wireless speciality networks (**"WSN**s") such as wireless personal area networks (**"WPAN**s"), Bluetooth, IoT networks, body area networks and wearables. Meanwhile ETSI developed new standards for connectivity within vehicles.

In addition, other organisations have developed new standards for particular connected technologies that implementers in the UK should also be aware of. For example, the Society of Automotive Engineer's Standard J2735 covers standardised messages to facilitate emergency breaking.

15. How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

In the UK as in other jurisdictions, technical standards which facilitate interoperability between connected devices mean that parties developing connected technologies which utilise a technology such as 5G or Bluetooth will need to consider patents which have been declared "essential" to those technologies – so-called standard essential patents (**"SEPs"**).

Any member of an SDO such as ETSI is required to declare any patent which it owns which is essential or potentially essential to one or more of the SDO's technical standards. A patent will generally be 'essential' either if the claimed invention of the patent must be used in order to comply with the standard or if commercially and practically it is the only way to comply.

If a patented technology becomes part of a technical standard and it is mandatory to implement the particular feature, the resulting SEP will be infringed by anyone implementing a solution which complies with the standardised technology.

Balancing the patent holder's monopoly rights against the need to ensure technologies can be implemented and prevent 'hold up' by a patent owner, the members of an SDO such as ETSI, in declaring their patent as standard essential, undertake to grant a licence to the SEP to any 'willing licensee' on 'fair, reasonable and non-discriminatory' (**"FRAND"**) terms.

Implementers of services or manufacturers of devices in the UK which use wireless connectivity technologies such as 5G or Bluetooth therefore need a licence to those patents declared essential to the relevant standard and which they must necessarily implement to comply with the standard.

Such licensing may be negotiated with patent holders individually, as has been the model for the mobile phone industry, or through patent pools where those are available, for example in the automotive industry or for IoT. As car manufacturers incorporate more cellular technology into vehicles, they are increasingly using technologies such as 5G or Bluetooth so that vehicles can communicate with the external environment, other vehicles and devices within them. In response to these changes, Avanci LLC has developed a licensing program whereby, for a fixed price per vehicle, it offers a licence to a 'pool' of patents owned by multiple patent holders and covering various core patents for wireless communications.

16. When negotiating agreements which involve mobile communications or other connected

technologies, are there any different considerations in respect of liabilities/warranties relating to standard essential patents (SEPs)?

When negotiating agreements which involve mobile communications or other connected technologies, there are different considerations in respect of liabilities/warranties relating to standard essential patents (**"SEPs"**).

Clauses in collaboration agreements which deal with IPR need to take account of SEPs just as any other patents. Indemnities need to take account of the risk of SEP infringement, as it will be difficult for a third party to have rights to use all SEPs which may be relevant to the technology, given the number of different SEP holders from whom licences need to be obtained. Depending on the technology used, the level of indemnity should take account of the threat of assertions, whether by established telco and tech companies which hold core patents for mobile communications or by 'non-practising entities' (**"NPEs"**) which hold relevant SEPs and engage in licensing campaigns to exploit those rights.

Agreements with suppliers therefore need to be clear as to which party bears the risk for royalty payments. This is particularly relevant in the case of connected and autonomous vehicles, where Avanci's licence program (see Question 15 above) is open only to vehicle manufacturers and not to suppliers.

Other clauses in agreements may need to reflect the likelihood that intellectual property rights (**"IPR"**) are likely to include SEPs. For example, in collaborations where there may be joint R&D and/or joint IPR, strategic decisions may need to be made as to the parties' appetite to engage with SDOs and seek to develop patents which may be declared standard essential.

17. Which body(ies), if any, is/are responsible for data protection regulation?

Data protection is primarily regulated in the UK by The Information Commissioner's Office (ICO), an executive non-departmental public body.

18. Please summarise the principal laws (present or impending), if any, that that govern data protection, including a brief explanation of the general purpose of those laws.

PRESENT

Principal laws	Brief description
The General Data Protection Regulation (2016/679) ("EU GDPR")	The EU GDPR enhances individuals' data protection and privacy rights and harmonises the data protection laws within the EU, aiming to ensure that personal data is handled responsibly by organisations and in accordance with fundamental privacy principles. The EU GDPR has extraterritorial effect and will apply to UK-based controllers and processors who: • are processing personal data in the context of activities of the controller or processor's establishment in the EU; or • offer goods or services to data subjects in the EU, or who monitor the behaviour of data subjects in the EU. There are also implications for UK controllers who have an establishment in the EEA, have customers in the EEA, or monitor individuals in the EEA. The EU GDPR still applies to this processing.
UK GDPR	The EU GDPR is retained in modified form in the United Kingdom ("UK") under the UK General Data Protection Regulation ("UK GDPR"). The key principles, rights and obligations of the UK GDPR remain the same as the EU GDPR. The UK GDPR also applies to controllers and processors based outside the UK if their processing activities relate to: • offering goods or services to individuals in the UK; or • monitoring the behaviour of individuals taking place in the UK. The UK has the independence to keep this framework under review. The UK GDPR sits alongside the Data Protection Act 2018 ("DPA 2018").
DPA 2018	The DPA 2018 initially set out permitted derogations and supplementary provisions to the EU GDPR, repealing and replacing the Data Protection Act 1998. The DPA now sits alongside and supplements the UK GDPR (for example, it provides the exemptions from the UK GDPR).
Law Enforcement Directive EU 2016/680 ("LED")	Part 3 of the DPA 2018 brought the LED into UK law. This complements the UK GDPR and sets out requirements for processing personal data by law enforcement authorities.
The Data Protection (Charges and Information) Regulations 2018	The Data Protection (Charges and Information) Regulations 2018 require every UK controller that processes personal information to pay a data protection fee to the ICO unless all the processing of personal data by the data controller is exempt processing. The information provided to the ICO is published on a register. These regulations determine the fees an organisation will need to pay in relation to data protection charges. There are three different tiers of fee and controllers are expected to pay between £40 and £2,900.
Freedom of Information Act 2000 ("FOIA")	FOIA provides public access to information held by public authorities. It does this in two ways: • public authorities are obliged to publish certain information about their activities; and • members of the public are entitled to request information from public authorities. FOIA covers any recorded information that is held by a public authority in England, Wales and Northern Ireland, and by UK-wide public authorities based in Scotland. Information held by Scottish public authorities is covered by Scotland's own Freedom of Information (Scotland) Act 2002.

Privacy and Electronic Communications Regulations 2003 ("PECR")	PECR are derived from European law. PECR implement European Directive 2002/58/EC, also known as 'the e-privacy Directive', which complements the general data protection regime and sets out more specific privacy rights on electronic communications. PECR cover: • marketing by electronic means, including marketing calls, texts, emails and faxes; • the use of cookies or similar technologies that track information about people accessing a website or other electronic service; • security of public electronic communications services; • privacy of customers using communications networks or services as regards traffic and location data, itemised billing, line identification services (e.g. caller ID and call return), and directory listings. The EU is in the process of replacing the current e-privacy law with a new e-privacy Regulation ("ePR"), to apply alongside the EU version of the GDPR. However, the ePR will not automatically form part of UK law as the UK has left the EU.
Environmental Information Regulations 2004 ("EIR")	The EIR provide public access to environmental information held by public authorities. They do this in two ways: • public authorities must make environmental information available proactively; and • members of the public are entitled to request environmental information from public authorities. The EIR cover any recorded information held by public authorities in England, Wales and Northern Ireland. Environmental information held by Scottish public authorities is covered by the Environmental Information (Scotland) Regulations 2004.
Network and Information Systems Regulations 2018 ("NIS Regulations")	The NIS Regulations intend to address the threats posed to network and information systems and therefore aim to improve the functioning of the digital economy. NIS Regulations concern 'network and information systems' and their security. These are any systems that process 'digital data' for operation, use, protection and maintenance purposes. NIS Regulations require these systems to have sufficient security to prevent any action that compromises either the data they store, or any related services they provide.
Investigatory Powers Act 2016 ("IPA")	The IPA provides a framework to govern the use and oversight of investigatory powers by law enforcement and the security and intelligence agencies. The IPA sets out the lawful acquisition of communications data which is the "who, where, when, how and with whom" of a communication but not the content (i.e. what was said). The IPA builds on, and supersedes parts of, the Regulation of Investigatory Powers Act 2000 ("RIPA"). There are limited exceptions to the prohibitions in the Investigatory Powers (Interception by Businesses etc. for Monitoring and Record-keeping Purposes) Regulations 2018 (SI 2018/356). The Act has recently been amended by the Investigatory Powers (Amendment) Act 2024 to widen government access to publicly available data and to communications data from telecoms companies for intelligence purposes.
Re-use of Public Sector Information Regulations 2015 ("RPSI")	RPSI relates to public sector information produced as part of a public task. Under regulation 3 public sector bodies have to publish a list of the main information they hold for the purpose of a public task. RPSI does not apply to information that would be exempt from disclosure under information access legislation (such as the DPA 2018 and FOIA).
Regulation (EU) 910/2014 on electronic identification and trust services for electronic transactions in the internal market ("eIDAS")	Following the UK's withdrawal from the EU, the eIDAS Regulation was adopted into UK law and amended by The Electronic Identification and Trust Services for Electronic Transactions (Amendment etc.) (EU Exit) Regulations 2019. In addition, the existing UK trust services legislation, The Electronic Identification and Trust Services for Electronic Transactions Regulation 2016 (SI 2016/696) was also amended. The UK eIDAS Regulations set out rules for UK trust services and establish a legal framework for electronic signatures, seals, time stamps, documents, registered delivery services and certificate services for website authentication, and also recognises equivalent services in the EU. Electronic trust services can be used in a number of ways to provide security for electronic documents, communications and transactions e.g. to help ensure that documents sent electronically have not been altered in any way and that the sender can be easily recognised. Electronic trust services allow for such security properties to be applied and then validated and thus help ensure confidence in the electronic transfer of information.
Retained EU Law (Revocation and Reform) Act 2023 ("REUL")	The Retained EU Law (Revocation and Reform) Act 2023 made significant changes to the domestic body of law previously called "retained EU law", now "assimilated law". It revoked provisions in 587 legislative instruments of EU-related origin, together with all retained directly effective EU law (for example, rights and obligations formerly conferred directly under EU treaties or directives) and various other principles of EU law as they applied in the UK. As a result, references in the UK GDPR and Data Protection Act to EU Treaty-derived "fundamental rights and freedoms" now refer to the Human Rights Act 1998. From May 2024, the REUL Act will also reduce the influence of EU decisions on domestic courts.
The Product Security and Telecommunications Infrastructure Act 2022 (PSTI)	The PSTI Act and Regulations made under it the PSTI (Security Requirements for Relevant Connectable Products) Regulations 2023) institute a UK consumer connectable product security regime. The product compliance regime outlines security requirements for manufacturers of in scope "smart" devices, such as internet-connected baby monitors, domestic appliances and smartphones. Current requirements concern default passwords, product information and product support periods. The full regime commenced on 29 April 2024.
Online Safety Act 2023 (OSA)	The OSA became law on 26 October 2023, but key parts are being implemented in phases through secondary legislation and Ofcom codes of practice. It is expected to govern 100,000 organisations of all sizes, including in the areas of social media, search engines and online advertising. The first phase, concerning duties on illegal harms, is likely to be finalised by the end of 2024. Some measures are currently in force – such as the requirement for organisations to update their terms of service to reflect users' rights to bring breach of contract claims. One key aim is to protect children by making organisations like social media platforms: • Remove illegal content quickly or prevent it from appearing in the first place. This includes removing categories of content like that promoting self-harm or bullying or hateful content; • Prevent children from accessing harmful and age-inappropriate content; • Enforce age limits and age-checking measures; • Ensure the risks and dangers posed to children are more transparent, including, for large organisations, by publishing risk assessments; and • Provide parents and children with clear and accessible ways to report problems online when they do arise. The duties depend on factors such as the size of the online service. Services will also need to: • Remove illegal content; • Remove content that is banned by their own terms and conditions; and • Empower adult internet users, for example with tools so that they can tailor the type of content they see. Ofcom has powers to take action against non-compliant organisations. Fines will be up to £18 million or 10 percent of annual global turnover, whichever is greater. Senior managers can face imprisonment under a host of new cyber offences, and Ofcom may also pursue service cessation orders.
Digital Markets, Competition and Consumers Act	This introduces a competition regime for the largest and powerful digital platforms including a mandatory code of conduct and merger control. It gives the Competition and Markets Authority (CMA) the power to designate undertakings with a link to the UK, and turnover of £1bn in the UK or £25bn globally, as having strategic market status (SMS) in respect of a digital activity and to impose conduct requirements on designated undertakings. The CMA will, following investigation, be able to intervene to promote competition where it considers that activities of a designated undertaking are having an adverse effect on competition through pro-competition interventions (PCIs). The Act also introduces a duty for designated undertakings to report certain mergers and to produce compliance reports. The CMA will be granted investigatory and enforcement powers. The first SMS designations are expected from mid-2025.

IMPENDING (as of June 2024)

Principal law	Brief Description
UK Data Protection and Digital Information Bill	The DPDI Bill aimed to alleviate the burden of compliance with the UK GDPR and its implementation in the UK Data Protection Act 2018 for organisations in the UK. The Bill included changes to UK GDPR plus digital verification services, smart data schemes, changes to PECR including greater fining powers and ICO reform (among others). The Bill was near completion in May 2024 when it was dropped as a result of the general election. Data protection reform may be renewed by the next government.

19. What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

Law(s)	Sanction
UK GDPR and DPA 2018	The ICO can take enforcement action by issuing enforcement notices (imposing fines or the suspension or cessation of processing), assessment notices (for a compulsory audit) or information notices (requiring the provision of information for investigation). There are two tiers of fines that can be imposed by the ICO: • A maximum fine of £17.5 million or 4 per cent of annual global turnover – whichever is greater – including for infringement of any of the data protection principles, rights of individuals or rules concerning restricted data transfers. • A maximum fine of £8.7 million or 2 per cent of annual global turnover – whichever is greater – for infringement of other provisions, such as administrative requirements of the legislation.
EU GDPR	The enforcement action that data protection regulators in EU Member States can take is generally similar to actions the ICO can take in the UK. There are two tiers of fines that can be imposed by data protection regulators in EU Member States: • A maximum fine of €20 million or 4 per cent of annual global turnover – whichever is greater – including for infringement of any of the data protection principles, rights of individuals or rules concerning restricted data transfers. • A maximum fine of €10 million or 2 per cent of annual global turnover – whichever is greater – for infringement of other provisions, such as administrative requirements of the legislation.
LED	In the UK, ICO fines for law enforcement authorities are subject to the same financial limits as under UK GDPR. In European member states, maximum fines are determined by member state law.
The Data Protection (Charges and Information) Regulations 2018	A fine of up to £4,350 (150% of the top tier fee) can be imposed by the ICO for failure to pay the data protection fee.
FOIA	The ICO does not have the power to fine a public authority under FOIA. However, failure to comply with an ICO enforcement notice may lead to prosecution and a fine of up to £5,000 in the magistrates' court and an unlimited fine in the Crown Court.
PECR	The ICO can impose a fine of up to £500,000 for breach of the PECR.
EIR	As under FOIA, the ICO has no direct power to fine. However, a controller who breaches the EIR and has been served with an enforcement notice can be prosecuted for failing to comply with a notice. This offence carries a maximum penalty of a £5,000 fine in the magistrates' court and an unlimited fine in the Crown Court.
NIS Regulations	The NIS Regulations set out a sliding scale of maximum financial penalties which can be imposed by the ICO: • £1 million – for any contravention that the ICO determines was not 'a material contravention'; • £8.5 million – for a 'material contravention which the ICO determines does not and could not have created a significant risk to, or significant impact on, or in relation to, the service provision by the OES* or RDSP*'; • £17 million – for a 'material contravention which the ICO determines has or could have created a significant risk to, or significant impact on, or in relation to, the service provision by the OES or RDSP'. *An OES is an 'operator of essential services', and an RDSP is a 'relevant digital service provider'.
IPA	Imprisonment for a term not exceeding 2 years, a fine, or both.
eIDAS	The ICO can take action for breaches of eIDAS, including by imposing fines of up to £1,000.

In addition, the DPA 2018 includes provisions for criminal offences related to data protection, including:

- unlawful obtaining, disclosing, or selling of personal data. It is a criminal offence to intentionally or recklessly obtain, disclose, or sell personal data without lawful authority. This offence can be punishable by a fine or imprisonment.
- re-identification of de-identified personal data. Re-identifying previously de-identified

personal data without lawful authority is a criminal offence, subject to fines or imprisonment.
- alteration of personal data to prevent disclosure. Knowingly altering, defacing, blocking, erasing, or destroying personal data with the intention of preventing its disclosure is an offence under the DPA 2018.

Offences committed by a person in an organisation

The DPA 2018 introduces the concept of "offences by bodies corporate." This means that if an offence under the DPA 2018 is committed by an organisation, such as a company, partnership, or government body, the organisation can be held criminally liable. This includes offences related to data protection principles, appointment of a data protection officer, etc. Criminal penalties in the DPA 2018 apply to processing under the LED by competent law enforcement authorities.

20. Do technology contracts in your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international element?

In relation to the EU GDPR, yes, especially as a result of the extraterritorial effect of the EU GDPR.

References to other third country data protection laws (such as the CCPA) are not typically included in contracts, unless they are directly applicable to the processing carried out as part of the services provided under the contract.

21. Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

As of June 2024, there is no single body responsible for the regulation of artificial intelligence (AI) in the UK.

The AI Policy Directorate, which sits within the Department for Science, Innovation & Technology, issues papers and guidance on the UK approach to AI regulation, but is not responsible for regulation. Instead, the Government will rely on existing regulators to manage AI development and deployment within their sector, to ensure (through existing powers) that AI is used safely and ethically. The Department for Science, Innovation & Technology issued Initial Guidance for Regulators in February 2024, which mentioned several key regulators who have already issued guidance on AI, including:

- The Advertising Standards Agency, which has issued guidance confirming that existing regulation on how advertisements are made applies to advertisements using AI;
- The Competition and Markets Authority, which has issued guidance detailing how end users need to be informed of the limitations of AI foundational models to maintain an environment of healthy competition;
- The Information Commissioner's Office, which has issued best practice guidance on data protection-compliant AI, and is engaging with the Government on further proposals for regulatory reform that will support the Government's pro-innovation approach to AI regulation;
- The Financial Conduct Authority, which in April 2024 issued a response to the Government's AI White Paper, outlining its strategy for promoting the safe and responsible use of AI in UK financial markets; and
- The Medicines and Healthcare products Regulatory Agency, which has published guidance on how AI systems can be used in healthcare and medical devices.

Certain other organisations in the UK are also working to develop standards and best practices for the use of AI, including the Alan Turing Institute. Such organisations may play an advisory role in future regulation of AI in the UK.

22. Please summarise the principal laws (present or impending), if any, that that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

As of June 2024, there are no laws dealing directly with artificial intelligence in the UK comparable with, for example, the EU's AI Act. Instead, the principal laws governing the deployment and use of AI are existing laws relating to issues such as data protection, equality and discrimination, intellectual property ownership and unfair competition, as well as certain sector-specific guidelines issued by existing regulators, as discussed in Question 21.

It seems likely that new laws and regulations, or modifications to existing laws and regulations, will be promulgated as the regulation of AI develops and evolves.

23. Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI?

No. However, the Department for Science, Innovation & Technology's recent White Papers have made extensive reference to Large Language Models (LLMs), and "Frontier AI" (which the Government defines as "highly capable general-purpose AI models that can perform a wide variety of tasks and match or exceed the capabilities present in today's most advanced models") was a key focus of the UK's AI Safety Summit in November 2023. The Government has made clear that it will not place any of the principles outlined in its White Papers so far on a statutory footing, to preserve a "pro-innovation approach" to AI, however it has indicated that position could change where the current framework requires supplementing in order to address issues arising from the development of Frontier or other highly capable AI systems. The UK position may change following the July 2024 General Election.

24. Do technology contracts in your jurisdiction typically contain either mandatory (e.g mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

No. Although template clauses to address AI clauses are emerging, they are not yet established. Issues or risks to consider when approaching such types of provisions include broader intellectual property licensing and ownership (including related warranty or indemnity protection), whether the AI will be consumer-facing, whether there is a sector-specific regulatory angle, and whether emerging regulatory frameworks (potentially including overseas regulation with extraterritorial application such as the EU AI Act) apply, and (where the contract relates to generative AI), what rights or prohibitions apply to the information that can be inputted to or used in conjunction with the relevant generative AI platform .

25. Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

Not as standard. As in Question 24, template clauses are emerging, but are not yet established. However, where contracting for AI systems, particularly ones which create outputs which may be subject to further commercial exploitation by either party, or be shared or published externally, the rights in and ownership of any materials generated should be carefully considered in contracting for the relevant AI systems.

26. What are the principal laws (present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

In principle, any person can launch a protocol, smart contract, ledger or blockchain in the UK. This is a technological endeavour which is currently completely unregulated in the UK.

When taking a broader interpretation of the question, the issue at stake is the *use and application* of blockchain and associated digital asset technology.

In the UK, the regulatory regime specifically covering digital assets (including tokens, cryptocurrencies, NFTs and new forms of organisational structures (e.g. Decentralised Autonomous Organisations ("**DAOs**")) is different to the EU's Markets in Crypto Assets ("**MiCA**") Regulation. MiCA treats "crypto assets" as an entirely new asset-class. In contrast, the UK's approach has been to treat some digital assets as within scope of the existing rules and others outside its perimeter. The Financial Services and Markets Act 2023 (and statutory instruments promulgated under it) will bring some digital assets within the perimeter in 2025, with others to follow later. In order to offer products and services in those assets inside the existing regulatory perimeter, a firm would need to be authorised and regulated in the usual way. The perimeter of current rules is blurred to an extent: it is possible that some firms which offer products and services outside the scope of traditional regulation still operate their business in a way which requires them to become authorised and regulated under, for example, Payment Services Regulation or the Electronic Money rules, or registered with the FCA for money laundering purposes (sometimes known as a VASP registration).

The FCA has focused its efforts on publishing information for consumers about the risks of dealing with digital assets and with unauthorised firms (e.g. those based outside the UK).

In the meantime, the Bank of England is in the final stages of launching a new "Digital FMI Sandbox". This will permit

firms which want to provide depository services for digital assets (other than unbacked spot cryptocurrencies) to do so within a ring-fenced regulatory environment. This environment will permit firms to conduct (some) business while the regulatory authorities determine what rules (a) need to be changed to permit that business to be conducted outside the Sandbox and (b) will be deemed not to apply to the firms while they are in the Sandbox. This project requires input from HM Treasury, the Bank of England, the PRA and the FCA.

A notable absentee from any current proposal is an update to the market abuse rules to cover digital assets specifically. In March 2024, the FCA announced that its strategy included amending the market abuse regime to include manipulation on and abuse of digital assets markets. This is likely to go hand-in-hand with bringing digital assets within the regulatory perimeter.

On the horizon, we can see the requirement for some brokers of crypto/digital assets to become authorised and regulated in the UK as trading venue operators. That process is something about which firms which may be affected should consider in short order, as obtaining those permissions is a lengthy process.

27. Please summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation of the general purpose of those laws.

Currently, search engines and marketplaces in the United Kingdom are primarily governed by general laws that apply to online services and information providers. Whilst there are no specific laws dedicated to search engines and marketplaces, the following legal frameworks are relevant:

- Electronic Commerce (EC Directive) Regulations 2002 (amended through the Electronic Commerce (Amendment etc.) (EU Exit) Regulations 2019 following Brexit) ("E-Commerce Regulations"): The E-Commerce Regulations apply to virtually every commercial website, including marketplaces which are considered "information society services". The E-Commerce Regulations impose certain obligations on marketplace operators, including the requirement to provide mandated information to users and have prescribed features and functions of the site relating to contract formation.
- Platform to Business Regulations (Retained Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services and corporate website users of online search engines (also known as the UK Platform-to-business Regulation or UK P2B Regulation) as amended by the Online Intermediation Services for Business Users (Amendment) (EU Exit) Regulations 2020, SI 2020/796 ("P2B Regulations"): The focus of the P2B Regulations is to regulate the relationship between business users and search engines and online intermediation services (such as marketplaces) that use them to sell products or services. The P2B Regulations seek to ensure that the platforms operated by these types of intermediaries deal with their business users fairly and in a transparent manner. The rules ban certain unfair practices, such as changing online terms and conditions without cause, and mandate transparency over the ranking of search results.
- Online Safety Bill (currently on its second reading passing through the report stage of the House of Lords): The Bill will make search engines legally responsible for protecting the online safety of their users, requiring that they remove harmful or illegal content quickly or prevent it from appearing in the first place.
- Advertising Standards: Those search engines or marketplaces that display advertisements must comply with advertising standards and endure that adverts on the platform meet the regulations set by the Advertising Standards Authority, such as the UK Code of Non-broadcast Advertising and Direct & Promotional Marketing, which is the rule book for non-broadcast advertisements, sales promotions and direct marketing communications.
- Data Protection Law: Those search engines or marketplaces that process personal data of users must comply with all applicable laws and regulations in the UK relating to privacy and the processing of personal data relating to data subjects located in the UK, including the UK General Data Protection Regulation (as defined in The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019), the Data Protection Act 2018, and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003).
- Consumer Protection Laws (including the Consumer Rights Act 2015 ("CRA") and

Consumer Protection From Unfair Trading Regulations 2008 ("CPRs"):Search engines and marketplaces must comply with the requirements set out in the CRA, including ensuring any consumer terms and notices comply with the requirements of fairness and transparency (this would include any "buyer" terms and conditions or rules that feature on a marketplace). In addition, platforms must comply with the requirements set out under the CPRs, which prohibit certain commercial practices (including the prohibition on acting contrary to the requirements of professional diligence and prohibitions on misleading actions or omissions and aggressive practices, as well as the list of practices that are in all circumstances considered unfair set out in Schedule 1 to the Consumer Protection from Unfair Trading Regulations 2008 and Schedule 18 of the Digital Markets Competition and Consumers Bill (DMCC) – which is yet to receive Royal Assent. These apply during the whole lifetime of a consumer-to-trader transaction (i.e. advertising, marketing, entry into the contract, performance and enforcement). The prohibition on acting contrary to the requirements of professional diligence requires traders to act with reasonable skill and care, commensurate with honest market practice and the general principle of good faith in their field of activity. The Government has begun a consultation to understand how both traders and consumers consider this general standard to apply across all consumer transactions on online platforms. Consumers also benefit from specific protections in areas like product safety and advertising standards, where the Government is also acting to ensure consumers are protected. For example, the UK Product Safety Review consultation (UKPSR) included proposals for ensuring online platforms take due care to identify and remove unsafe products, provide consumers with accurate information on higher risk products and cooperate with regulators. The Government intends that the practical application of the professional diligence requirements should complement area-specific obligations such as those proposed in the UKPSR.

28. Please summarise the principal laws (present or impending), if any, that govern social media, including a brief explanation of the general purpose of those laws?

Social media platforms in the UK are primarily governed currently by general laws that apply to online services and information providers. Whilst there are no specific laws dedicated to social media platforms, the following legal frameworks are relevant:

- The Statutory Code of Practice ("Code"): The Code for providers of online social media platforms was published in accordance with Section 103 of the Digital Economy Act 2017. The Code provides guidance for social media platforms. It sets out actions that the Government believes social media platforms should take to prevent bullying, insulting, intimidating and humiliating behaviours on their sites. The Code is directed at social media platforms, but is also relevant to any sites hosting user-generated content and comments, including review websites, gaming platforms, online marketplaces and the like. The Code does not affect how illegal or unlawful content or conduct is dealt with.
- Online Safety Bill ("Bill"): The Bill, currently on its second reading passing through the report stage of the House of Lords, will makes social media platforms legally responsible for protecting the online safety of their users, in particular minors. It will protect users by requiring social media platforms to: remove illegal content quickly or prevent it from appearing in the first place, enforce age limits and age-checking measures, and provide parents and children with clear and accessible ways to report problems online when they do arise. The Bill will also empower adult internet users with tools so that they can tailor the type of content they see and avoid potentially harmful content. Ofcom, as regulator, will have powers to take action against companies who do not follow their new duties.
- Electronic Commerce (EC Directive) Regulations 2002 (amended through the Electronic Commerce (Amendment etc.) (EU Exit) Regulations 2019 following Brexit) ("E-Commerce Regulations"): The E-Commerce Regulations apply to virtually every commercial website including social media platforms (which are considered "hosting services", since they typically host and display user generated content). The E-Commerce

Regulations impose certain obligations on social media platforms, including the requirement to provide mandated information. The E-Commerce Regulations seek to protect social media platforms from liability caused by content posted by users.

- Platform to Business Regulations (Retained Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services and corporate website users of online search engines (also known as the UK Platform-to-business Regulation or UK P2B Regulation) as amended by the Online Intermediation Services for Business Users (Amendment) (EU Exit) Regulations 2020, SI 2020/796 ("P2B Regulations")): The focus of the P2B Regulations is to regulate the relationship between business users and online intermediation services (e.g. marketplaces, social media platforms etc) and search engines. The P2B Regulations seek to ensure that the platforms operated by these types of intermediaries deal with their business users fairly and in a transparent manner. The rules ban certain unfair practices, such as changing online terms and conditions without cause, and mandate transparency over the ranking of search results.
- Advertising Standards: Social media platforms that display advertisements must comply with advertising standards and ensure adverts meet the regulations set by the Advertising Standards Authority, such as the UK Code of Non-broadcast Advertising and Direct & Promotional Marketing ("CAP Code"), which is the rule book for non-broadcast advertisements, sales promotions and direct marketing communications. The CAP Code covers many different types of advertising in social media, from the more traditional 'paid-for' ads to advertorials and affiliate marketing. The CAP Code requires that all marketing, including that on social media, is legal, decent, honest and truthful, and contains general rules and sector-specific rules that marketers must comply with. The CAP Code also requires that marketing communications are obviously identifiable as such and sets out further rules around influencer marketing.
- Data Protection Law: Social media platforms that process personal data of users must comply with all applicable laws and regulations in the UK relating to privacy and the processing of personal data relating to data subjects located in the UK, including the UK General Data Protection Regulation (as defined in The Data Protection, Privacy and Electronic Communications (Amendments etc) (EU Exit) Regulations 2019), the Data Protection Act 2018, and the Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2426/2003).
- Consumer Protection Laws (including the Consumer Rights Act 2015 ("CRA"): Social Media platforms must comply with the requirements set out in the CRA, including ensuring any consumer terms and notices comply with the requirements of fairness and transparency (this would include any platform terms of use, for example).

29. What are your top 3 predictions for significant developments in technology law in the next 3 years?

1. Further developments in laws and regulations governing the use of artificial intelligence.

Laws and regulations around AI are already developing rapidly in the UK and elsewhere. It is possible this trend will continue, particularly if there is a change of government following the July 2024 General Election. For example, the Labour Party has indicated it may be more amenable to additional intervention on AI compared with the incumbent Conservative administration, which has maintained a more laissez-faire "pro-innovation" approach.

It seems likely that future regulation will focus on the responsible use of highly capable generative AI and LLMs. There is likely to be further debate around the open source development of LLMs (which may run the risk of complicating or evading conventional regulatory oversight).

We are also likely to see increased international standardisation of AI regulation and standards, or the establishment of a body having international oversight, particularly as the EU's AI Act comes into force, and/or through bodies such as the OECD, UN and initiatives such as the AI Safety Summits first initiated by the UK Government in London in 2023, and most recently hosted by South Korea.

The UK has already entered into bilateral agreements with the likes of the USA and South Korea around cooperation on AI model testing and controls, and further international

agreements of this type may also feature in the UK's approach.

2. Further developments in laws and regulations governing the "Web3" space, especially blockchain and cryptoassets.

As with AI, more regulation seems likely in the Web3 space to keep up with the rapid development of products in this area, particularly cryptoassets. Although some of the fervour around certain cryptoassets, for example NFTs, seems to have abated, Web3 and, in particular, the decentralisation of the Internet, is still an area into which a huge amount of investment is being poured, and which has significant complexity and accordant risk, making it ripe for further regulation. The UK Government (HM Treasury) set out its final proposals for a regulatory regime for cryptoassets in October 2023, confirming its intention to bring a number of crypto activities under regulatory scrutiny. The Financial Services and Markets Act 2023 (**FSMA 2023**), which will facilitate stablecoins and cryptoassets being brought into financial services regulation, received Royal Assent on 29 June 2023.

3. Developments in privacy law to keep pace with the greater use of technology by government bodies and law enforcement.

As government agencies and law enforcement make greater use of technology (in particular, AI, facial recognition, etc), it seems probable that there will be increased concerns around how these technologies (particularly AI) affect and potentially impinge on individuals' privacy rights and civil liberties. This may lead to the UK Courts ruling on the legality of such use of technology by the Government and other public services as well as by corporations such as tech giants and/or social media companies.

30. Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

It is increasingly common for customers to request sustainability provisions in their contracts, particularly when procuring business critical technology systems. In particular, UK Government entities, certain large UK corporates, and certain financial institutions (e.g. prominent banks) may be subject to extra regulatory scrutiny around their sustainability/net zero commitments.

Often, technology vendors' public-facing websites have sections that outline their commitments to sustainability (sometimes as part of their ESG reporting), often containing extensive reporting data. For technology vendors with a global presence (e.g. cloud services 'hyperscalers'), this data will usually be presented at a global operational level, so it may be difficult to glean UK-specific information from such websites without requesting further information from the vendors.

Technology vendors typically resist inserting sustainability commitments at a contractually binding level with individual customers. As an alternative, they may agree to provide more fulsome information than that contained on their public websites for review, including country-specific data and/or scorecards/reviews from external sustainability ratings agencies such as EcoVadis.

Where the customer is a public sector body, or a large corporate or financial institution, it may be more feasible to negotiate contractual level commitments around sustainability from technology vendors.

Contributors

Joe Stephenson
Partner
joe.stephenson@shoosmiths.com

Paul Nightingale
Principal Associate
paul.nightingale@shoosmiths.com