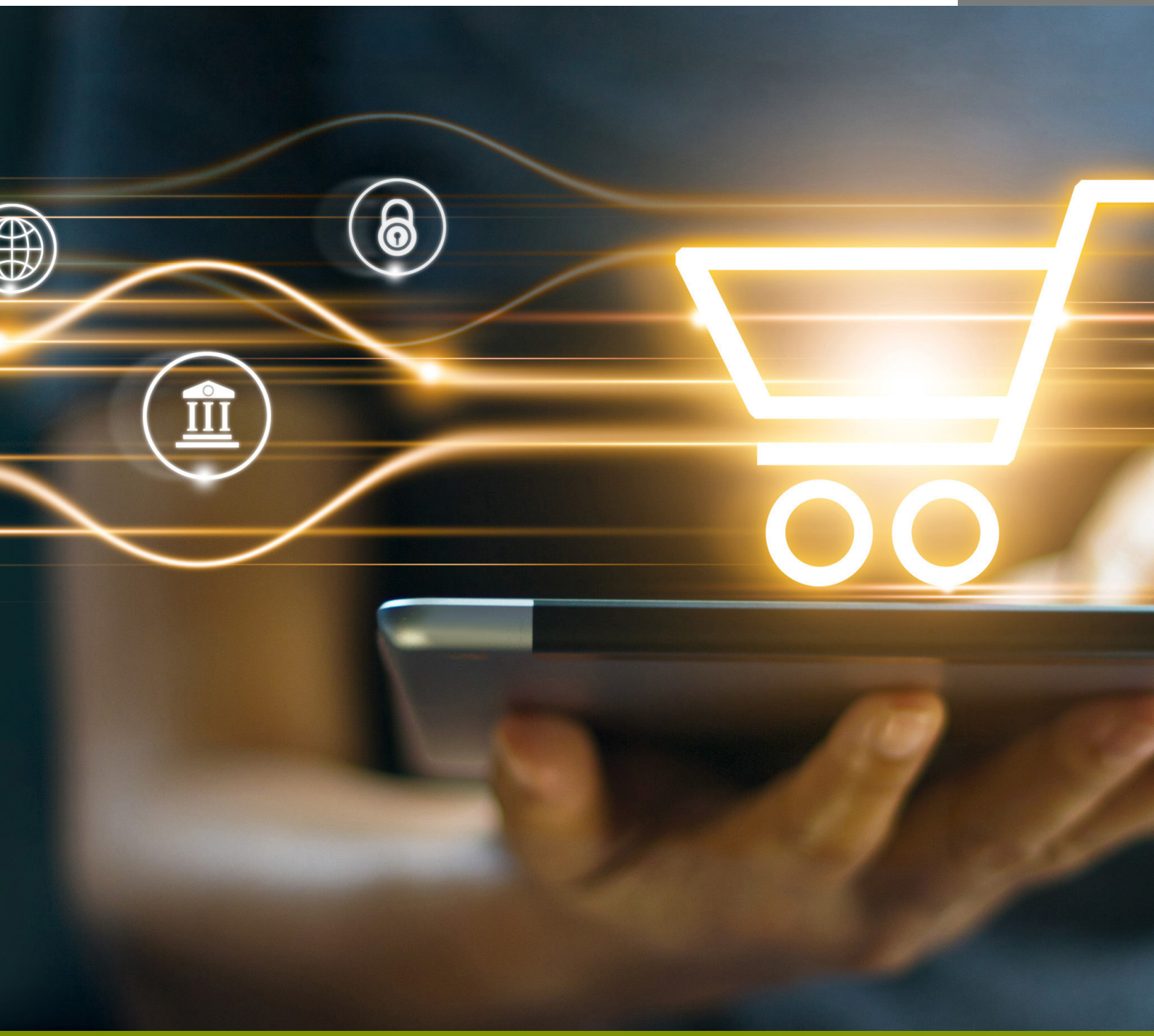
KEMP IT LAW

IT Law at the Apex

DIGITAL COMMERCE



White Paper

Current Issues in Digital Commerce Regulation

Richard Kemp, Deirdre Moynihan, Chris Kemp

May 2021

CURRENT ISSUES IN DIGITAL COMMERCE REGULATION
TABLE OF CONTENTS

TABLE OF TABLES

CURRENT ISSUES IN DIGITAL COMMERCE REGULATION

A. INTRODUCTION

1. **Introduction, scope and purpose**. This white paper is a collection of the individual blogs we have written as introductory and companion pieces to the segments of our Digital Commerce webinar on 28 April 2021:

   - Top tips for digital business contracting (Section B);
   - UK payment services regulation – data and cryptoassets: the developing landscape (Section C);
   - Recent digital commerce legislation (1): the Platform to Business Regulation (Section D);
   - Recent digital commerce legislation (2): over the top services and the EECC (Section E);
   - Recent digital commerce legislation (3): video sharing platforms (Section F); and
   - Upcoming platform regulation: the EU Digital Services Act and UK Online Harms Bill (Section G).

B. CONTRACTING FOR DIGITAL SERVICES: TOP TIPS FOR B2B AND B2C AGREEMENTS

2. **Introduction**. This is a short companion piece to our webinar on 28 April 2021 on Digital Commerce. It overviews some of the questions about contracting for digital services that we are most frequently asked to look at.

3. **Clickwrap or browsewrap?** It's clickwrap when the user scrolls down the terms and conditions or terms of service and clicks the 'I accept' button. So long as the provider keeps a record of acceptance in their system then clickwrap is generally recognised under English law as meeting the formal requirements for contract formation - offer, acceptance, consideration and communication of acceptance to the offeror.

   in the browsewrap case, the user is simply notified that continued use of the website or service constitutes acceptance of the terms and conditions or terms of service, but the user takes no positive action. In this case, the UK Law Commission has stated that there is no valid acceptance so there is unlikely to be a contract, whether in the B2C or B2B scenario.

   However, even if there is no binding contract, some terms may be effective by notice - for example copyright or other IP licensing terms, and some liability terms that are effective when brought to the notice of the user.

   In practice whether to use clickwrap or browsewrap is a balance between managing conflicting priorities - the extra resource to ensure the 'I accept' and record retention function in the provider's system and perceived user resistance against the risk of unenforceable contractual terms.

4. **How do we know the person clicking has authority?** There's a famous New Yorker cartoon of a dog at their computer workstation turning to a friend and saying "On the Internet, nobody knows you're a dog". This neatly illustrates the difficulty of standard website terms that say "where you accept for the Customer, you confirm that you have authority to bind the Customer to these terms and conditions" and/or "if you do not have authority to bind the Customer do not click 'I agree'".

To coin Joseph Heller, another famous New Yorker, there's a bit of a Catch 22 here: if the person accepting does not have authority then the customer can argue it isn't bound by the terms he or she purportedly signed up to; and also there's no basis (apart from perhaps misrepresentation) to take action against the person accepted as there's no contract.

Again, in practical terms this is a risk management matter - what's the worst that can happen for the provider if the person purportedly signing does not have authority? If the provider can adopt through later action- for example payment - or you could get a written signature from the customer by someone actually or apparently in authority, then this risk is more manageable.

5. **What about e-signatures?** The UK legal and regulatory framework for electronic signatures is based on the 2014 EU eIDAS regulation. It's gaining traction quickly at the moment, particularly in data trust frameworks and other digital data driven ecosystems. Essentially, it's in three parts or layers:

   - first, it regulates the requirements for **e- signatures** (and e- time stamps, e-documents etc.) as digital data associated with other digital data that the signatory uses to sign and gives them legal admissibility, broadly in the same way as written signatures;
   - second, it introduces **Trust Services** ensuring certainty in the digital transactions concerned by confirming the validity of the underlying e-signature, Etc;
   - thirdly, it establishes a system of Qualified Trust Service Providers - entities who effectively guarantee authenticity. (There are 17 Qualified Trusted Services Providers in the UK at the moment, including Barclays, BT, Digidentity, Entrust, Experian, RBS, Royal Mail and Verizon).

6. **What security duties apply to digital commerce transactions?** Whilst there is no single source of security duties in the digital space, **digital commerce businesses**:

   - as ***data controllers*** must take appropriate technical and organisational measures ('**ATOMs**') to ensure security appropriate to the risk (Article 32 GDPR);
   - as ***public electronic communications service ('ECS') providers***, in the language of telecoms regulation, must take ATOMs to "safeguard the security of that service" (Regulation 5, PECR 2003) – note that the e-privacy regulation is still making its way through the legislative process and is likely to impose stricter duties when passed and to the extent it's implemented in the UK;
   - as ***cloud and other relevant digital service providers***, must take appropriate and proportionate measures to manage security risks (Regulation 12, NIS Regs 2016);
   - ***accepting card payments***, must comply with the PCI DSS (Payment Card Industry Data Security Standard);
   - may also be subject to ***sector specific security regulation*** depending on their particular sector; and
   - may be subject to civil (? statutory) liability for ***breach of duty of care***.

7. **Do we need to use data encryption?** Data encryption is not legislatively or regulatorily prescribed, but is recognised in article 32(1)(a) GDPR as a way of taking appropriate technical and organisational measures to ensure security, so may be helpful evidence as positive steps taken to manage security risk.

On the other hand, note that the US EARN IT and LAED Acts, if enacted, could ban providers from offering end to end encryption without a built in means of decryption for law enforcement; and that the EC Council Resolution of 24th November 2020 on encryption expressly notes the law enforcement challenges of encryption and that preserving lawful access for law enforcement is essential.

8. **Do we have to accept when the cloud service provider insists on broad suspension rights?** This question needs to be looked at from both the provider's and the customer's perspectives. From the customer's standpoint a provider right to suspend could in some cases be viewed as a back door to termination without proving fault. The customer will view these terms particularly closely especially when this sort of term is in a contract that covers a service or system that is mission critical for the customer.

   However, the provider will need to reserve its rights in its customer agreements to take down offending material on notice in order to preserve its intermediary liability immunities under the e-Commerce Regulations (hosting, caching and mere conduit). In order to preserve these rights, it is likely to need to include some suspension rights in order to be in a position to comply with these statutory duties.

   In general terms, there's a practical balance to be struck here between not hamstringing necessary provider actions (on the one hand) and not making it too easy to suspend on the other.

9. **Are we free to choose the law that governs the contract?** Generally:

   - In B2B contracts, the parties will usually be able to agree between themselves the governing law and jurisdiction terms that apply, so long as the clause is correctly drafted;
   - In B2C contracts involving the UK and the EU however, consumers:
     - when ***claiming***, can choose to claim in their or the provider's country;
     - when ***being claimed against***, may only be sued in their own country.

   However, the underlying background law is a thicket of rules, both in the business and consumer spaces, consisting of a mix of international conventions and common law. Brexit has inevitably had an impact on the EU based regulations that the UK signed up to and it will take some time for these to be clarified.

C. UK PAYMENT SERVICES REGULATION – DATA AND CRYPTOASSETS: THE DEVELOPING LANDSCAPE

10. **Introduction**. In this short piece, we overview the main aspects of payment services regulation in the UK. We also explore two 'hot topic' trends: data and cryptoassets. **Para 10** looks at the rules at a high level. **Para 12** takes a closer look at the two data-focused payment services introduced by the Second Payment Services Directive and briefly explores the impact of Open Banking. **Para 13** looks at how regulators are starting to bring cryptoassets within the payment services regulatory perimeter.

11. **UK payment services regulation – overview**. Two Statutory Instruments underpin the regulation of payment services in the UK:

    - the Payment Services Regulations 2017 (the "**PSRs**"); and

- the Electronic Money Regulations 2011 (the "**EMRs**").

These regulations started life as the UK implementations of the underlying EU directives – the Second Payment Services Directive and the Second Electronic Money Directive. Now, post-Brexit transition period, they are part of retained EU law in the UK.

At a high level, the PSRs require providers of payment services to be authorised or registered with the FCA. They also establish a regulatory regime payment services providers must follow. The EMRs create an authorisation and registration framework for issuers of electronic money. Beyond the PSRs and the EMRs themselves, there is a range of helpful regulatory guidance:

- **PERG.** A useful first port of call is the Perimeter Guidance Manual in the FCA Handbook (otherwise known as "**PERG**"). PERG contains separate chapters on the PSRs (15) and the EMRs (3A) and contains guidance on the scope of the rules. PERG helps to answer the scoping question, which is typically: do I need to be authorised or registered with the FCA to do [x]?
- **The Approach Document.** The FCA's Approach Document sets out the FCA's approach to implementing the PSRs and the EMRs.
- **EBA 'level three material'.** This is a range of non-legislative material produced by the European Banking Authority (the "**EBA**"), including its guidelines, opinions and recommendations. Post-Brexit transition period an important point will be to check the FCA website to confirm the FCA's compliance position on this material.

12. **Trend 1: data in payment services – the PSRs and Open Banking**

With the regulatory background in mind, our first trend: the ever-expanding role of data in payment services. Beyond the general increase in the importance of data in digital commerce, there are two specific structural drivers for this in the payment services world:

- The first is the creation of new data-driven payment services in the PSRs.
- The second is Open Banking.

a) ***The creation of new data-driven payment services in the PSRs***. The PSRs created two new data-driven payment services:

- Account Information Services (or "**AISs**"); and
- Payment Initiation Services (or "**PISs**").

AISs are defined (in the PSRs) as "online service[s] to provide consolidated information on one or more payment accounts held by the payment service user with another payment service provider or with more than one payment service provider".

PISs are defined (in the PSRs) as "online service[s] to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider".

AISs and PISs are interesting because they take advantage of other rules in the PSRs which require banks to share user account data with third party services providers (assuming the user consents, of course).

AISs and PISs are nothing new – the PSRs have been in force since January 2018. But what we are seeing now – three years down the line – is a flourishing industry sector enabled by the regulatory framework underpinned by the PSRs. This sector is increasingly interested in harnessing the vast amounts of data that flow through its systems.

b) ***Open Banking***. The second structural driver is Open Banking. Precisely what is meant by "Open Banking" varies by jurisdiction. But a helpful general definition is provided by the Basel Committee on Banking Supervision:

> Open Banking is "the sharing and leveraging of customer-permissioned data by banks with third party developers and firms to build applications and services, including for example those that provide real-time payments, greater financial transparency options for account holders, marketing and cross-selling opportunities."[1]

Open Banking is relatively well developed in the UK. This is thanks in large part to a major investigation by the UK Competition and Markets Authority ("**CMA**") into the retail banking sector in the mid-2010s. The CMA's investigation uncovered several areas of concern in the sector, primarily around the way the UK's largest retail banks were not transparent about the customer data they held.

At the end of its investigation, the CMA proposed a number of remedies. The key one for our purposes was the "open banking remedy", which required large UK retail banks to develop and adopt open API banking standards to make their data more accessible to customers and third-party service providers.

c) ***Data in payment services – practical points***. A number of practical points emerge from these trends:

- First, data is getting more important. Entities involved in payments structures where data is exchanged should ensure their contracts capture dataflows accurately. They should grant and take licences appropriately.
- Second, given the pace of change in the sector, entities should consider whether their important data contracts have enough flexibility to cover potential future use cases of data as well as current ones.

d) ***'Bonus' trend – payment services regulation and GDPR***. The relationship between payment services regulation and GDPR is something of a 'bonus' trend here: it will not come as a surprise to privacy lawyers that much of the user account data shared in the provision of AISs and PISs is personal data for the purposes of GDPR.

A key point here is to bear in mind how the PSRs and the GDPR fit together. There is some friction, particularly around:

- the appropriate GDPR lawful basis of consent;
- the concept of consent itself, as the PSRs concept is slightly different from the GDPR standard; and

[1] Basel Committee on Banking Supervision, *Report on open banking and application programming* interfaces (November 2019), p. 4., here: https://www.bis.org/bcbs/publ/d486.pdf.

- 'silent party' data (silent parties being natural persons whose data is processed by a payment service, but who are unaware of the processing – e.g. a 'payee' in a payment services application).

The European Data Protection Board's Guidance on the interplay between payments rules and GDPR from December 2020 is a useful starting point here.

13. **Trend 2: cryptoassets**

a) ***Introducing stablecoins***. Our second trend is that payment services regulation is starting to grapple with the wild west of cryptoassets.

This trend begins with an emerging class of cryptoassets called stablecoins. Stablecoins are a class of cryptoasset which aim to maintain a stable value. Stablecoins can achieve this in a number of ways, but the most common are:

- to peg their value to a stable 'real world' asset, like USD or gold; or
- to have their value determined by an algorithm.

In this respect, stablecoins are unlike other cryptoassets. Other cryptoassets are typically characterised by significant price volatility – making them prime candidates for speculative investment, but less useful as a stable, reliable store of value. Stablecoins, by contrast, have clear real-world uses – for instance as a cash-like holding assets used to store value pending investment decisions.

For this reason, coupled with their burgeoning popularity[2], stablecoins are the next step on the regulatory frontier for payment services. Their rapid growth poses a number of issues regulation would look to address, including: systemic risk, if an important stablecoin failed; the risk that consumers are mis-sold complex – perhaps even nonsensical – financial products; and distortive competitive advantage versus traditional financial products, if the regulatory burden faced by stablecoin users is artificially low.

b) ***HM Treasury's stablecoin consultation paper***. All this is the background to the UK Treasury's consultation paper on stablecoin regulation from January 2021, which sets out a number of regulatory proposals, based in large part on the existing regime for payment services under the PSRs and the EMRs.

At this stage, the Government's intention is only to regulate currency/asset-backed stablecoins. Not algorithmic stablecoins, which are spared for the time being. The proposals touch on a number of points:

- An authorisation or registration regime for certain market participants.
- A number of new regulated activities, including creating, issuing and destroying stablecoins.
- Other prudential requirements like capital and liquidity requirements.

The Government's proposals are still in the early stages of the regulatory process. The consultation closed in mid-March and the Treasury is still reviewing the responses.

[2] See e.g. this Bloomberg article: *Crypto's Shadow Currency Surges Past Deposits of Most U.S. Banks*, here: Crypto's Shadow Currency Surges Past Deposits of Most U.S. Banks - Bloomberg.

c) ***Stablecoin regulation – practical points***. But there are several practical points to bear in mind at this stage:

- First, in the coming years a greater number of cryptoassets – stablecoins and potentially other varieties – will fall within the regulatory perimeter. This is going to make payment services regulation relevant for a greater number of digital commerce businesses.
- Second, although regulators are beginning to tackle cryptoassets, we are still very much in a Galapagos islands world where cryptoassets come in a great many shapes and sizes. This makes it more important for market participants to diligence cryptoassets properly. By diligence we mean: understanding contractual T&Cs, redemption and exchange rights and the relationship between the cryptoasset and the underlying asset (if any).
- Third, market participants should ensure they understand both their own role and other participants' roles in the structure. This is particularly important where formal regulatory authorisation is not required for a given activity – but registration with or notification to a regulator is necessary. In practice these points are sometimes missed.

D. RECENT DIGITAL COMMERCE LEGISLATION (1) – THE PLATFORM TO BUSINESS REGULATION

14. **The P2B Regulation**. The Online Intermediation Services Regulation (2019/1150), commonly called the 'Platform to Business' or P2B Regulation) came into effect on 12 July 2020 and represents the first time that the EU has specifically sought to comprehensively regulate online platforms, search engines and corporate websites. This note is a brief overview of the main provisions of the P2B Regulation.

15. **Online intermediation services ('OISs') under the P2B Regulation**. OIS is defined at Art. 1(2) P2B Regulation. An OIS will be covered if:

a) it is an Information Society Service (see point 5 below);

b) it allows:

> "business users[3] to offer goods or services to consumers, with a view to facilitating the initiating of direct transactions between those business users and consumers, irrespective of where those transactions are ultimately concluded"; and

c) it is provided to business users on the basis of contractual relationships between the ISS provider and business users offering goods or services to consumers.

16. **Online search engines ('OSEs') under the P2B Regulation**. OSE is defined at Art 1(5) P2B Regulation as:

> "a digital service that allows users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information

[3] Defined at Art.1(1) as "any private individual acting in a commercial or professional capacity who, or any legal person which, through online intermediation services offers goods or services to consumers for purposes relating to its trade, business, craft or profession".

related to the requested content can be found."

17. **Corporate website users ('CWUs') under the P2B Regulation**. The P2B Regulation also covers and 'corporate website users' defined at Art 1(7) as:

> "any natural or legal person which uses an online interface, meaning any software, including a website or a part thereof and applications, including mobile applications, to offer goods or services to consumers for purposes relating to its trade, business, craft or profession."

18. **What is an Information Society Service ('ISS') ?** The key definition for digital commerce regulation in the UK and EU is that of 'information society service' ('**ISS**') under the EC's E-Commerce Directive 2000/31 of 8 June 2000 (the '**E-CD**')[4]. ISS are summarised in the E-CD as any service (i) normally provided for a remuneration (which is construed broadly), (ii) at a distance, (iii) by means of electronic equipment for the processing … and storage of data, and (iv) at the individual request of a recipient of the service".[5]

19. **Examples of covered and non-covered OIS**. OISR 2019 Recital 11 gives as examples of covered OIS:

> "online e-commerce marketplaces, including collaborative ones on which business users are active, online software applications services, such as application stores, and online social media services … It should also not be relevant whether those transactions between business users and consumers involve any monetary payment or whether they are concluded in part offline."

Recital 11 also states that the following are not covered:

a) non-business user peer-to-peer services without the presence of business users;

b) pure B2B services which are not offered to consumers;

c) non-transactional advertising services;

d) SEO services;

e) ad-blocker services;

f) "technological functionalities and interfaces that merely connect hardware and applications should not be covered by this Regulation" However, where "such functionalities or interfaces can be directly connected or ancillary to certain [OIS] … the relevant [OIS] providers should be subject to transparency requirements related to differentiated treatment based on these functionalities and interfaces."

g) online payment services as "inherently auxiliary to the transaction for the supply of goods and services to the consumers concerned."

---

[4] as implemented under UK law by the EC Directive Regulations 2002 SI 2002/2013 as amended (the '**UK Regs**')

[5] Recital 18 of the ECD provides examples of economic activities that do and do not fall within the definition.

Activities falling within the definition include: (i) selling goods online, (ii) offering online information or commercial communications (as an economic activity), (iii) providing tools allowing for search, access and retrieval of data (as an economic activity), (iv) transmission of information via a communication network, (v) providing access to a communication network, (vi) hosting information provided by a recipient of the service, (vii) video on demand and (viii) provision of commercial communications by electronic mail.

Activities not falling within the definition include: (i) delivery of goods, (ii) off-line service provision, (iii) broadcasting (because it is not provided at individual request) and (iv) personal use of email.

20. **The P2B Regulation applies to the platform (OIS) provider's Ts&Cs where 'unilaterally determined'**. Where a business user offers goods or services to its consumer customers through the platform's OIS, then the requirements of the P2B Regulation will apply to the contractual terms and conditions between the platform provider and its business users that are 'unilaterally determined' by the platform (OIS) provider. Recital 14 adds colour to what is meant by 'unilaterally determined':

> "Whether the terms and conditions were unilaterally determined should be evaluated case by case on the basis of an overall assessment. For that overall assessment, the relative size of the parties concerned, the fact that a negotiation took place, or that certain provisions thereof might have been subject to such a negotiation and determined together by the relevant provider and business user should not, in itself, be decisive."

21. **What are the main requirements of the P2B Regulation for OIS – Articles 3 and 4?** The requirements of the P2B Regulation in relation to OIS terms and conditions are many, prescriptive and granular. Terms that are non-compliant with the P2B Regulation are generally null and void. The main requirements are that the Ts&Cs must:

a) ***generally:***

- be drafted in plain intelligible and specific and avoiding misleading language;
- be easily available for business users at pre-contractual and all other stages of the relationship; and
- ensure that the identity of the business user providing the services via the OIS is clearly visible;

b) ***during relationship lifecycle:***

- include information on any additional distribution channels and affiliate marketing programmes by which the platform provider can market goods and services offered by business users;
- include details of most favoured nation and price parity provisions;
- include the main parameters determining ranking (relative prominence of goods or services) and the reasons for the relative importance of those parameters
- include a description of the type of ancillary services offered via the platform and whether and if so how the business user can also offer its own ancillary goods and services;
- be transparent as to the economic, commercial or legal reasons for differences in treatment of services offered by the platform provider and the business user;
- include general information regarding intellectual property rights of business users; and
- set out the technical/contractual access the business user will have to personal or other data provided by business users or consumers;

c) ***as to change in terms, termination, suspension, etc:***

- generally notify business users of changes to the terms and conditions by reasonable and proportionate notice of no less than 15 days and which allows the business user to terminate before notice expiry;

- include information about when business users can terminate the contractual relationship with the platform provider;
- provide business users with a statement of reasons for any restriction or suspension of platform availability for individual services;
- generally provide business users with a reasoned notice of no less than 30 days for termination of the platform services (subject to exceptions including repeated breach, illegal content, product safety, counterfeiting, fraud, malware, spam, data breaches, other cyber security risks or suitability of services for minors);
- state that grounds will be given for decisions to suspend, terminate or restrict service provision; and
- set out post-termination technical/contractual access to the data the business user provides or generates.

d) ***as to complaints and disputes:***[6]

- include relevant information about access to and functioning of internal complaint handling systems; and
- set out the identity of two or more mediators to resolve disputes with business users about their services.

22. **Special rules regarding interfaces**. By Art 7 P2B Regulation, additional rules are apply to ***technical interfaces*** affecting business user that are directly connected or ancillary to using the platform concerned. Art. 7 requires the platform provider to include in its Ts&Cs a 'description of the main economic or legal considerations' for 'differentiated treatment' for those services offered as between the business user (on the one hand) and the platform or any business users that the platform controls (on the other).

23. **What are the main requirements of the P2B Regulation for OSEs – Article 5?** The main requirements applicable to OSEs are set out in Article 5. Briefly they require the OSE provider to set out:

- the main parameters that, individually or collectively, are most significant in determining ranking;
- an easily and publicly available description of relative importance of those main parameters;
- where the main parameters make it possible to influence ranking through direct or indirect remuneration paid by business users or corporate website users, a description of those possibilities and the effects of such remuneration; and
- how a corporate website user can review a notification received from a third party that has led to the OSE provider altering the ranking order or delisting a particular website

[6] These rules do not apply to enterprises employing less than 50 persons and whose turnover or balance sheet is less than €10m.

E. RECENT DIGITAL COMMERCE LEGISLATION (2) – OVER THE TOP SERVICES AND THE EUROPEAN ELECTRONIC COMMUNICATIONS CODE

24. **Introduction**. Until a couple of years ago, it was a vexed question whether 'over the top' ('**OTT**') services – communications services bypassing telcos and other telecoms gatekeepers and provided directly to internet users – were caught by EU telecoms regulation. Then the *Google Gmail* and *Skypeout* cases in June 2019 settled that webmail and other OTT services which did not involve calling from or to a normal phone number were generally outside the net.

    This was seen as giving OTT providers a bunk up they didn't merit and the balance was redressed by the new European Electronic Communications Code, which builds on the underlying technical definitions to bring some OTT services back within the net. Here, what has emerged as 'number-independent interpersonal communications services' will be subject to light touch regulation. In the UK, the new rules have got caught up in Brexit and most will not come into effect before the end of this year, so OTT service providers still have some time to review how they're impacted by the new rules. This short piece explores the twist and turns.

25. **Definition of Electronic Communications Service ('ECS') under the UK Communications Act 2003 (CA)** . In the UK, S.32(2) CA defines ECS as:

    > "a service consisting in, or having as its principal feature, the conveyance by means of an electronic communications network [('**ECN**')} of signals, except in so far as it is a content service"

26. **The CA and EU telecoms law**. The CA was passed in part to implement the 2002 EU telecoms regulatory package which included the EU Framework Directive 2002/21 ('**FD**'). The CA's Explanatory Notes[7] state (at p.218) that s.32(2) CA is derived from Article 2(c) FD which in turn defines ECS as:

    > "service normally provided for remuneration which consists wholly or mainly in the conveyance of signals on [ECNs], including telecommunications services and transmission services in networks used for broadcasting, but exclude services providing, or exercising editorial control over, content transmitted using electronic communications networks and services; it does not include information society services … ***which do not consist wholly or mainly in the conveyance of signals on [ECNs]***". (emphasis added)

27. **The *Google Gmail* case.**[8] Google operated Gmail, a web based email service that did not itself provide internet access. The German utilities regulator, the BNetzA, decided under German law that Gmail was a telecommunications service (defined similarly to ECS under Article 2(c) FD) and accordingly that Google was required to register Gmail with the BNetzA.

    Google disputed the decision on the grounds that Gmail ***did not consist wholly or mainly in the conveyance of signals on ECNs*** because the signals were conveyed not by Google but by the email senders' and recipients' internet access providers and then over open internet networks.

    The German appeal court referred a number of questions to the European Court of Justice. As set out in paragraph 26 of the ECJ judgment, these included:

    > "whether Article 2(c) [FD] must be interpreted as meaning that a web-based email service which does not itself provide internet access, such as the Gmail service provided by Google, constitutes a service which

[7] http://www.legislation.gov.uk/ukpga/2003/21/pdfs/ukpgaen_20030021_en.pdf

[8] *Google LLC* v *Bundesrepublik Deutschland* (C-193/18) EU:C:2019:498 (13 June 2019), referred to as the *Google Gmail* case in this note. See judgment here.

> ***consists wholly or mainly in the conveyance of signals on [ECNs]***, having regard to the electronic processing which the provider of that service supplies via its email servers, on the one hand, by assigning to the email addresses the IP addresses of the corresponding terminal devices and, on the other hand, by uploading to or receiving from the open internet the data packets relating to the emails".

In its judgment on 13 June 2019, the European Court of Justice ('**ECJ**') agreed with Google's view, holding:

> "that Article 2(c) of the [FD] must be interpreted as meaning that a web-based email service which does not itself provide internet access, such as the Gmail service provided by Google, ***does not consist wholly or mainly in the conveyance of signals on [ECNs]*** and therefore does not constitute an [ECS] within the meaning of that provision" (paragraph 41 of the judgment).

The case clarified that Gmail and similar 'over the top' ('**OTT**') services were not ECSs within the FD.

28. **The *SkypeOut* case**.[9] By contrast, the ECJ had given another judgment a week earlier (on 5 June 2019) on the interpretation of Article 2(c) FD in the *SkypeOut* case. Here, SkypeOut was an extra, paid for feature of Skype's service that enabled Skype users to make outbound calls to a land line or mobile number using Voice over Internet Protocol ('**VoIP**'). In return for payment from its customers, Skype was contractually responsible for the SkypeOut VoIP service. Skype had also entered into interconnection agreements with fixed and mobile network providers under which it paid them charges for terminating SkypeOut calls on those providers' networks. In these circumstances the ECJ found that SkypeOut was an ECS:

> "Article 2(c) [FD] must be interpreted as meaning that the provision, by a software publisher, of a feature offering a VoIP service which allows the user to call a fixed or mobile number covered by a national numbering plan from a terminal via the PSTN of a Member State constitutes an [ECS] within the meaning of that provision, provided that, first, the software publisher is remunerated for the provision of that service, and, second, the provision of that service involves the conclusion of agreements between that software publisher and telecommunications service providers that are duly authorised to send and terminate calls to the PSTN" (paragraph 49 of the judgment).

29. **The European Electronic Communications Code ('EECC')** . The 2002 EU telecoms package was replaced by a new framework from 21 December 2020. Part of the new framework is EU Directive 2018/1972 establishing the EECC. Under the EECC, the definition of ECS is expanded to include in addition to the old definition under Art 2(c) FD (s.32(2) CA in the UK) new definitions including 'interpersonal communications services'.

30. **'Interpersonal communications services' ('ICS')** . By EECC recital 17 and Article 2(5), ICS are services:

> "normally provided for remuneration that enable interpersonal and interactive exchange of information, covering services like traditional voice calls between two individuals but also all types of emails, messaging services, or group chats"

The 'interactivity' requirement means that the service "allows the recipient of the information to respond" so ICS do not cover "linear broadcasting, video on demand, websites, social networks, blogs, or exchange of information between machines".

---

[9] *Skype Communications Sàrl* v *Institut belge des services postaux et des télécommunications* ('**IBPT**') C-142/18 (5 June 2019), referred to as the *SkypeOut* case in this note. See judgment here. The case is also referred to in the Practical Law case report mentioned at footnote 4 above.

As in other EU-based legislation using the 'information society service' definition, the 'normally provided for remuneration' requirement is broad and includes indirect remuneration, like access to data or advertising, as well as direct remuneration.

ICS are defined as either 'number-based' ('**NB-ICS**') or 'number-independent' ('**NI-ICS**'). NB-ICS are ICS that connect, or enable communication, with one or more telephone numbers from national and international numbering plans (EECC, recital 18 and Article 2(6). NI-ICS are ICS that do not connect, or enable communication in that way (EECC recital 18 and Article 2(7). Further, ICS may also be publicly available or not, with different rules applying (effectively as a 2x2 matrix: NB/NI-ICS x publicly/non-publicly available).

31. **Consequences of ICS falling within the EECC**.

a) ***Generally***: Under the EU framework, all providers of ECNs and ECSs are subject to a general authorisation regime. In the UK, this is Ofcom's General Conditions.[10] Under the new (EECC) regime, NI-ICS are expressly stated not to be subject to the general authorisation regime:

> "Contrary to the other categories of [ECNs and ECSs] as defined in this Directive, [NI-ICS] do not benefit from the use of public numbering resources and do not participate in a publicly assured interoperable ecosystem. It is therefore not appropriate to subject those types of services to the general authorisation regime" (EECC, Recital 44; operative provision – Article 12(2));

b) ***NI-ICS***: NI-ICS will however be subject to a number of requirements set out in EECC, Part III (Services), Title III (End-User Rights) at Articles 98 to 116. These exclude the requirement to provide access to emergency service calling and caller location information (Article 109).

For non-publicly available NI-ICS, they just include basic duties not to discriminate as to terms of access or use based on the end-user's nationality or place of residence or establishment (Art. 99) and to respect the EU Charter of Fundamental Rights and general principles of EU law (Art. 100).

Where NI-ICS are publicly available and (generally in that case) provided to consumers, microenterprises (headcount <10, t/o <€2m), small enterprises (headcount <50, t/o <€10m) or not for profits, Title III imposes further requirements.

c) ***NB-ICS***: unlike NI-ICS, NB-ICS are subject to the general authorisation regime, along with other requirements like publicly available NB-ICS are subject to more extensive requirements (Ofcom's General Conditions in the UK), including emergency calls (Art 109), public warning system (Art 110) and directory enquiries (Art 112).

32. **EECC: UK, Brexit and Covid**. The implementation date for the EECC was 21 December 2020 and so before the end of the Brexit transition period on 31 December 2020. The UK therefore accepted the requirement to transpose the EECC into English law (see DDCMS Consultation Paper, p.5) and this was done by regulations made on 2 December 2020.[11] DDCMS consulted on EECC implementation and in its 22.07.20 response to the public consultation paper stated (p.42) that:

> "COVID-19 has brought significant challenges to communications providers including higher demand for their services and the need to prioritise support for vulnerable customers. Therefore, providers are likely to

[10] General Conditions of Entitlement, Ofcom, 4 January 20201

[11] The Electronic Communications and Wireless Telegraphy (Amendment) (European Electronic Communications Code and EU Exit) Regulations 2020. (SI 2020/1419), effective from 21 December 2020.

need additional time to make the necessary changes to their systems and processes to comply with the new rules being introduced from the Directive. In light of this, on 7 May 2020, Ofcom stated that it will allow providers at least 12 months from the date of its statement to make the new rights available to customers."

Ofcom published its statement 'Implementing the new EECC'[12] on 17 December 2020 pushed out the deadline further to 17 December 2021, with other changes coming in in 2022:

"most of the new rules come into effect in December 2021, with contract information and right to exit rules coming into effect in June 2022 and new switching and porting rules in December 2022" (para 3.44).

So, OTT services providing NB-ICS in the UK still have some time to review how they're impacted by the new rules.

F. RECENT DIGITAL COMMERCE LEGISLATION (3) – VIDEO SHARING PLATFORMS

33. **Introduction**. The last couple of months of 2020 saw a flurry of regulatory activity around broadcasting in the UK, with:

a) the transposition into UK law (mainly) on 1 November 2020 of the revised AVMS Directive[13] (point 2 below);

b) the Brexit transition period ending on 31 December 2020 and consequential Brexit-related broadcasting changes came into force (point 3); and

c) Ofcom publishing a series of new guidance notes (point 6).

34. **The revised AVMS Directive and the UK AVMS Regs**. The Audiovisual Media Services Regulations, SI 2020/1062, (the '**AVMS Regs'**) [14] transposed the revised AVMS Directive into UK law (mainly) on 1 November 2020. Broadly, the AVMS Regs:

a) remove the requirement that audio-visual content must be 'TV-like' to be regulated;

b) introduce the concept of 'dissociability' (separateness) between services;

c) increase the regulatory burden on video on demand ('**VOD**') services; and

d) bring video sharing platforms ('**VSPs**') within scope from 6 April 2021.

35. **Brexit: the UK BAEE Regs and the ECTT**. The UK BREXIT regulations on broadcasting (the '**BAEE Regs**')[15] apply from 31 December 2020 and make certain Brexit-related changes to the pre-2021 UK regulatory regime. At high level, they effectively change the UK's television broadcasting authorisation system from a country of ***origin*** to a country of ***destination*** system, requiring television services available in the UK to be licensed and regulated by Ofcom.

[12] Statement: Implementing the new European Electronic Communications Code (ofcom.org.uk)

[13] Revised AVMSD (2018/1808 of 14 November 2018) amending the original AVMS Directive (2010/13/EU of 10 March 2010), together here the '**AVMSD**'.

[14] The Audiovisual Media Services Regulations 2020 (legislation.gov.uk) SI 2020/1062

[15] The Broadcasting (Amendment) (EU Exit) Regulations 2019 (SI2019/224)

They also implement the European Convention on Transfrontier Territory (the "**ECTT**")[16] so that broadcasters in ECTT States will not need a licence from Ofcom to broadcast into the UK, in effect (and subject to local law) retaining the country of origin principle for ECTT countries.

36. **The AVMSD and UK CA – core definitions: TLCS (linear), ODPS (non-linear) and VSPs**. The core definitions under the **AVMSD** of 'television broadcasting' (linear AVMS) and 'on-demand' AVMS (non-linear AVMS) have been translated into UK law as 'television licensable content service' ('**TLCS**' – linear) by s.232 Communications Act 2003 ('**CA**')[17] and 'on-demand programme service' ('**ODPS**' – non-linear) by s.368A CA. Video-Sharing Platform ('**VSPs**') are brought under regulation for the first time, at ss.368S to 368Z13 CA. Essentially, UK regulated TLCS must be licensed before service starts whilst UK regulated ODPS and VSPs are notifiable in advance but not licensable.

37. **Coming into force of the new VSP rules**. The new rules on VSPs came into effect on 6 April 2021. Existing UK-established VSPs have until 6 May 2021 to notify. Other VSPs must notify Ofcom of their intention to launch a UK-regulated VSP service at least 10 working days before services launch.

38. **Ofcom guidance, etc**. Ofcom published guidance on VSPs in October 2020[18] and a statement on who needs to notify on 10 March 2021.[19] It is currently consulting on guidance for VSPs on measures to protect users from harmful material.[20] its draft ODPS guidance.[21]

39. **VSPs in scope**. By s.368S CA, five criteria must be met for Ofcom to regulate a VSP. The VSP must be a service:

    a) where provision of ***videos to members of the public*** is 'the principal purpose' or an essential functionality of the service; and

    b) provided ***by means of an electronic communications network*** (i.e. including the internet); and

    c) provided ***on a commercial basis***; and

    d) where the ***person providing it***:

        (i) does not have general control over what videos are available on it, but

        (ii) does have general control over the manner in which videos are organised[22] on it; and

[16] European Convention on Transfrontier Television . Confusingly, not all EU member states are ECTT states – Denmark, Greece, Ireland, Luxembourg, the Netherlands and Sweden for example are EU, but not ECTT states

[17] Communications Act 2003

[18] 'Regulating video-sharing platforms: A guide to the new requirements on VSPs and Ofcom's approach to regulation' (21 October 2020);

[19] 'Video-sharing platforms: who needs to notify to Ofcom?'

[20] 'Video-sharing platform guidance: Consultation on guidance for VSP providers on measures to protect users from harmful material'. The consultation began on 24 March 2021 and ends on 2 June 2021.

[21] 'On-demand programme services: who needs to notify to Ofcom?' The consultation began on 31 March 2021 and ends on 26 May 2010. The current guidance dates from 24 November 2020 and is: ODPS - guidance notes on how to notify an ODPS to Ofcom and ODPS providers - statutory rules and non-binding guidance

[22] By s.368S(2)(c)(ii) CA "organised" includes "being organised automatically or by way of algorithms, in particular displaying, tagging and sequencing".

e) where that person is ***under the jurisdiction of the UK for the purposes of the AVMSD***. The jurisdiction requirements are complex.[23] Section 4 (pages 19 and 20) of Ofcom's 'who needs to notify' guidance (see footnote 7) is helpful in uncluttering the definition.

40. **Dissociability**. A feature of the revised AVMSD is generally to define a particular service (whether TLCS, ODPS or VSP) as 'all or any dissociable part' of that service, and this definition has been ported across to the CA via the AVMS Regs.

    It raises the possibility that a service with dissociable elements may be split and regulated under more than one head. Examples for and against dissociability are given in the revised AVMSD (at recital 3). "Stand-alone parts of online newspapers featuring audio visual programmes or user generated videos" may be dissociable, whereas a service that "should be considered to be merely an indissociable complement to the main activity as a result of the links between the audio visual offer and the main activity" will not. Recital 6 states that "where a dissociable section of a service constitutes a [VSP] service for the purposes of [the AVMSD], only that section should be covered by that directive and only as regards programmes and user generated videos".

    In the absence of specific guidance on how dissociability may apply between services that could possibly be characterised as TLCS, ODPS and/or VSPs, providers will need to make their own evidenced decisions against the criteria in the revised AVMSD.

41. **Regulation post notification**. The main purpose of the new VSP regulatory regime is to protect consumers who engage with VSPs from the risk of viewing harmful content. Providers must have in place appropriate measures to protect under-18s from material which might impair their physical, mental or moral development, and to protect the general public from criminal content and material likely to incite violence or hatred. Services will also need to make sure standards around advertising are met. The statutory framework sets out a list of measures which providers must consider taking, as appropriate, to secure the required protections.

42. **Penalties**. The statutory regime is enforceable by Ofcom through penalties of up to £250,000 or 5% of qualifying turnover if greater. Ofcom can also serve enforcement notices, which it can enforce through civil proceedings for an injunction, specific performance or any other appropriate remedy.

G. UPCOMING PLATFORM REGULATION: THE EU'S DIGITAL SERVICES ACT AND UK'S ONLINE HARMS BILL

43. **The trend to increasing scrutiny**. The activities of platform operators are increasingly subject to scrutiny from users and regulators alike trying to maintain the "surface tension" between freedom of choice and speech and concerns around online bullying, racist remarks, copyright infringement, sale of counterfeit products or other illegal behaviour.

    This section summarises proposed "policing the internet" regulation in the EU and the UK at a high level and focusses on the new proposals to update the existing "safe harbours" for caching, hosting and mere conduit.

[23] They are also rather confusing. Although similar to those for TLCS, they do not have the equivalence effect of the ECTT that certain TLCS have. Pre-Brexit, the ODPS rules were based on the AVMSD and so would have been similar to the VSP rules had they been in force then. However, the BAEE Regs have changes the ODPS jurisdiction requirements to the provider's 'head office' being in the UK and editorial decisions about the service being take in the UK.

The EU's Digital Services Act

44. **Introduction.** The EU's draft Digital Services Regulation (the DSA) is the European Commission's proposed regulation applicable to online intermediary services. Its aim is to protect consumers and their fundamental rights while also requiring platform operators offering services in the EU to act in a transparent and accountable manner.

Not all intermediaries are subject to the same rules. The number of obligations and requirements increases as the intermediary serves more consumers with an ever-increasing set of services. The proposed ramp up in obligations means that e.g., Facbook or Twitter will be subject to a higher number of more onerous obligations than e.g., BT as your internet service provider, as illustrated by the following table of obligations (see here).

The goal is to ensure that those providers who are used by most individuals are subject to additional rules intended to increasingly more onerous obligations including transparency as to how the intermediary makes decisions (e.g., to explain why content has been removed, reporting on removal of content, informing users if there are restrictions on use of data and what filtering or moderation techniques are used, and disclosures around ad display and targeting to name a few).

Very large platforms will also be required to analyse systemic harm from the use of their platforms, to allow for audits, to share parameters of decision-making methodologies, to publish details of all ads posted on the platform, to appoint a compliance officer and implement codes of conduct and crisis response protocols. The European Commission will also have regulatory oversight.

Table 1: Proposed DSA Obligations

Obligation	Intermediary services (network infrastructure) (cumulative obligations)	Hosting services (cloud and webhosting services) (cumulative obligations)	Online platforms (online marketplaces, app stores, collaborative economy platforms and social media platforms) (cumulative obligations)	Very large platforms (platforms reaching more 45 million consumers in Europe) (cumulative obligations)
Transparency reporting	●	●	●	●
Requirements on terms of service due account of fundamental rights	●	●	●	●
Cooperation with national authorities following orders	●	●	●	●
Points of contact and, where necessary, legal representative	●	●	●	●
Notice and action and obligation to provide information to users		●	●	●
Complaint and redress mechanism and out of court dispute settlement			●	●

Obligation	Intermediary services (network infrastructure) (cumulative obligations)	Hosting services (cloud and webhosting services) (cumulative obligations)	Online platforms (online marketplaces, app stores, collaborative economy platforms and social media platforms) (cumulative obligations)	Very large platforms (platforms reaching more 45 million consumers in Europe) (cumulative obligations)
Trusted flaggers			•	•
Measures against abusive notices and counter-notices			•	•
Vetting credentials of third party suppliers ("KYBC")			•	•
User-facing transparency of online advertising			•	•
Reporting criminal offences			•	•
Risk management obligations and compliance officer				•
External risk auditing and public accountability				•
Transparency of recommender systems and user choice for access to information				•
Data sharing with authorities and researchers				•
Codes of conduct				•
Crisis response cooperation				•

Although asymmetrical, the new rules in the DSA are likely to require most intermediaries to take steps to implement the new rules and to update and refresh existing practices and procedures to meet the new requirements of the DSA. This is likely to be at significant cost to businesses in the short-medium term. The sanctions for non-compliance, however, are significant: up to 6% of the annual global income.

45. **The "exceptions" to liability.** Given the imposition of more responsibility on intermediaries, the preservation of the safe harbours against liability is welcomed. Helpfully, the DSA re-baselines the exceptions, first introduced in the E-Commerce Directive, to remove the differences in approach between member states and clarifies that voluntary monitoring by intermediaries does not disapply the exceptions – a point which was not necessarily uniformly applied under the national implementations of the E-Commerce Directive.

46. **Legislative process.** The DSA is currently under review by the European Parliament Internal Market and Consumer Protection committee.

The UK's Online Harms Bill

47. **Current status**. Unlike the EU, the UK government has not yet prepared a draft of the Online Harms Bill. However, the government's intention is to create a new duty of care to (a) prevent the proliferation of illegal content and activity online and (b) ensure that children who use the services are not exposed to harmful content. The duty of care will apply extra-territorially to search engines and service providers anywhere in the world whose users are located in the UK and who host user-generated content and/or facilitate online interaction between users (including public communication channels and services (online instant messaging services and closed social media groups) where users expect a greater degree of privacy). An additional, smaller subset of tech companies will be obliged report on what they are doing to tackle activity and content that is harmful to adults.

48. **The duty of care** will require companies to "take reasonable steps to keep users safe, and prevent other persons coming to harm as a direct consequence of activity on their services". The list of online harms currently within scope is as follows (see here):

Table 2: Online Harms Currently Within Scope

Harms with a clear definition	Harms with a less clear definition	Underage exposure to legal content
Child sexual exploitation and abuse.	Cyberbullying and trolling.	Children accessing pornography.
Terrorist content and activity.	Extremist content and activity.	Children accessing inappropriate material (including under 13s using social media and under 18s using dating apps; excessive screen time).
Organised immigration crime.	Coercive behaviour.	
Modern slavery.	Intimidation.	
Extreme pornography.	Disinformation.	
Revenge pornography.	Violent content.	
Harassment and cyberstalking.	Advocacy of self-harm.	
Hate crime.	Promotion of Female Genital Mutilation (FGM).	
Encouraging or assisting suicide.		
Incitement of violence.		
Sale of illegal goods/ services, such as drugs and weapons (on the open internet).		
Content illegally uploaded from prisons.		
Sexting of indecent images by under 18s (creating, possessing, copying or distributing indecent or sexual images of		

Harms with a clear definition	Harms with a less clear definition	Underage exposure to legal content
children and young people under the age of 18).		

Companies who are within scope will be expected to comply with regulatory codes and proactively compliance with the new duty of care. This may include taking prompt action following complaints of illegal activity, providing support (via a third party) for users who have suffered harm, preventing dissemination of known terrorist content and supporting the police and prosecutors in pursuing criminals.

A failure to comply may result in a fine of up to the higher of 10% of global turnover or £18 million.

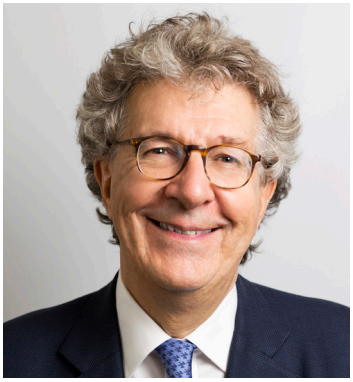
49. **The "exceptions" to liability.** The government has reviewed the safe harbour exceptions provided by the E-Commerce Directive. In its opinion, the current regime is "not the most effective mechanism for driving behavioural change by companies. The existing liability regime only forces companies to take action against illegal content once they have been notified of its existence." It's likely, therefore that the UK government will introduce specific monitoring obligations for limited categories of illegal content and while increasingly the responsibility imposed on the service provider – details on the specifics are scant at the time of writing.

50. **Comment**. Although both the UK and the EU are seeking to tighten the rules applicable to online intermediaries, the approach is different – the EU is adopting an asymmetrical model imposing specific and defined obligations, with broad exceptions whereas the UK is proposing to capitalise on the existing English law concept of a "duty of care", with more onerous monitoring obligations and a potentially narrower set of exceptions. This potential for divergence, made possible by Brexit, may result in complex compliance issues for companies in an area where technology changes frequently and where those companies may need to comply with both UK and EU rules in a way not envisaged pre-Brexit.

Richard Kemp, Deirdre Moynihan and Chris Kemp
Kemp IT Law,
London,
May 2021

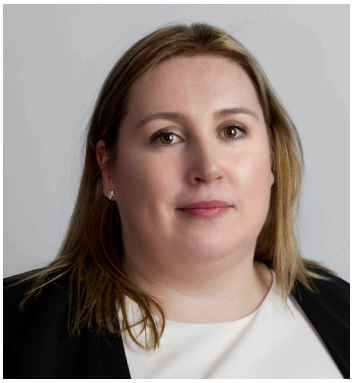
KEMP IT LAW

IT Law at the Apex



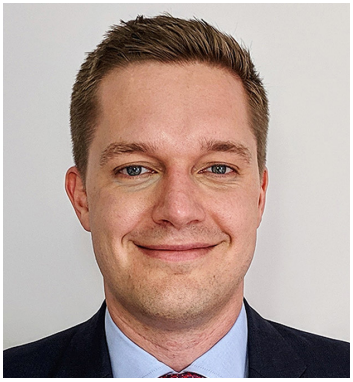
Richard Kemp
Partner

T: 020 3011 1670
M: 07932 695 615
richard.kemp@kempitlaw.com



Deirdre Moynihan
Partner

T: 020 3011 1627
M: 07710 395 460
deirdre.moynihan@kempitlaw.com



Chris Kemp
Associate

T: 020 3011 1678
M: 07710 396 071
chris.kemp@kempitlaw.com