Appendix A: the relevant legal framework

Introduction

1. In this appendix we will describe at a high level the legislative and regulatory landscape relevant to our consideration of mobile ecosystems in the UK. This is intended as a brief, factual description of the key applicable frameworks rather than a substantive assessment of the extent to which those laws and regulations apply in mobile ecosystem markets.

2. This appendix is structured in the following thematic way:

   - first, we provide an overview of sector-specific legislation and regulation currently in force that we consider to be most relevant to mobile ecosystems;
   - second, we set out a broad summary of generally-applicable laws of relevance, including laws on data protection and privacy, competition, and consumer protection;
   - third, we briefly describe the role of standard setting and self-regulation, where relevant to this study; and
   - finally, we provide a brief update on various proposed changes to the legal and regulatory landscape (relevant to mobile ecosystems) that we anticipate coming into force within the next few years.

Specific legislation and regulation relevant to mobile ecosystems

3. This section summarises some of the relevant legislation and regulations relevant to the operation of mobile ecosystems.

Platform to Business Regulation

4. On 12 July 2020, the EU Regulation on platform-to-business relations (the P2B Regulation)[1] on promoting fairness and transparency for business users of online platforms and search engines became directly applicable in EU Member States (including in the UK, as part of the Transition Period following the UK's exit from the EU).[2] When the Transition Period ended on 31

[1] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.
[2] The P2B Regulations also impose certain obligation on providers of Online Search Engines; however, those provisions are of less direct relevance to the main matters considered in this study.

December 2020, the EU law version of the P2B Regulation was retained in UK law, with limited amendments largely to make it UK-centric.

5. The P2B Regulation applies to online intermediation service (OIS) providers – that is, services which connect businesses to their consumers, such as online search engines, consumer marketplaces and social media platforms.[3] The key requirements of the P2B Regulation include obliging platform providers to:

- ensure terms and conditions are transparent; business users of the OIS are given sufficient notice of any changes and can terminate their contract;
- tell business users at or before they are delisted, suspended or terminated from the service and the reasons why;
- inform business users in advance of the main parameters used to determine ranking, their relative importance, as well as any action businesses can take to influence the ranking, such as remuneration or accepting additional obligations;
- act in a transparent manner and set out the considerations for any differential treatment the provider might give in respect of goods and services it offers compared to those offered by the business users;
- provide business users with a description of the scope, nature and conditions of their access to and use of certain categories of data, for example online reviews and ratings; and
- explain the legal, economic or commercial grounds for any restrictions imposed by the OIS on the ability of business users to offer goods or services to consumers under more favourable conditions through other sales channels.

6. The P2B Regulation is also supported with mechanisms for dispute resolution. It aims to create a fair, transparent and predictable business environment for businesses and traders when using online platforms to offer services to consumers. In order to give effect to these dispute resolution mechanisms, the UK government made the Online Intermediation Services for Business Users (Enforcement) Regulations 2020 (the Enforcement Regulations) (which also came into force on 12 July 2020).[4] The Enforcement Regulations provide

[3] However, an 'ad exchange', ie a business selling to other businesses, would not be within scope as it is not a platform which allows business users to offer direct transactions to consumers.
[4] The Online Intermediation Services for Business Users (Enforcement) Regulations 2020, SI 2020/609.

that a failure of a provider of OIS to comply with Article 3 (terms and conditions), Article 4 (restriction, suspension and termination) or Article 8 (specific contractual terms) of the P2B Regulation is a breach of an obligation owed to a business user, such that, where loss or damage is caused to the business user, it may bring a civil action against the OIS provider in respect of that loss or damage.[5] The Enforcement Regulations also set out the powers of the court in relation to an application for an appropriate remedy.

UK cybersecurity laws

7. This section provides a brief overview of the key cybersecurity laws in the UK. These are:

- **The Computer Misuse Act 1990**: this legislation creates various cyber offences relating to computers, such as criminalising unauthorised access to computer material with or without intent to commit further offences; unauthorised acts with intent to impair the operation of a computer; and unauthorised acts causing or creating the risk of serious damage. However, unlike what follows below, the 1990 Act does not inherently create security obligations on businesses.

- **The Communications Act 2003:** this seeks to ensure the security and integrity of the public electronic communications networks (PECN) and public electronic communications services (PECS) by requiring providers to take appropriate technical and organisational measures to manage risks to the security of PECN and PECS, including measures to prevent or minimise the impact of security incidents on end users and on the interconnection of PECN. It creates further obligations on PECN and PECS providers to notify Ofcom of security breaches with a significant impact. Where providers contravene the requirements of the 2003 Act, Ofcom may take enforcement action which can result in the imposition of a penalty not exceeding £2 million.

- **The Telecommunications (Security) Act 2021:** this amends the Communications Act 2003 by establishing a new security framework, including new security duties on PECN and PECS providers and new powers for the Secretary of State to make regulations and issue codes of practice. It includes provisions strengthening Ofcom's regulatory powers, allowing them to enforce the new framework. In particular, the new framework increases the maximum penalty amount to 10% of turnover.

[5] The Enforcement Regulations also provide that qualifying organisations and associations (as defined in Article 14(1) of the P2B Regulation) may bring court proceedings for an appropriate remedy to secure compliance by OIS providers with relevant requirements of the P2B Regulation.

The 2021 Act also introduces new national security powers for the Government to impose, monitor and enforce controls on PECN and PECS providers' use of designated vendors' goods, services and facilities.

- **The Privacy and Electronic Communications (EC Directive) Regulations 2003 (the PECR, implementing ePrivacy Directive 2002/58/EC):** the PECR include security obligations in respect of personal data that apply to PECS providers. The PECR require PECS providers to take technical and organisational measures to ensure the security of their services by restricting who can access personal data and protect the way it is stored or transmitted. The measures taken by PECS providers can be audited by the Information Commissioner's Office (ICO) and, where contraventions are discovered, providers can be subject to monetary penalties. Further details on the PECR are provided later in this Appendix.

- **The Network and Information Systems Regulations 2018** (NIS Regulations) implemented the EU Network and Information Systems Directive into UK law, imposing obligations on operators of essential services (OES) and relevant digital service providers (RDSPs):

    - OES covers organisations operating services deemed critical to the economy and wider society including energy, water, healthcare and digital infrastructure;

    - RDSPs includes those providing search engines, online marketplaces or cloud computing services (regulation 8).

  The NIS Regulations require OES and RDSPs to take appropriate and proportionate technical and organisational measures to manage risks and to prevent the data they hold or the services they provide being compromised. The measures taken and level of security must be appropriate to the risk posed. Compliance with the NIS Regulations is monitored through inspections conducted or arranged by designated competent authorities/the ICO. Regulation 18(6) details the maximum financial penalties, based on the materiality of the breach.

- **The Data Protection Act 2018:** also contains important elements relating to cybersecurity. These are covered in more detail below.

General law

8. This section provides a brief description of the legal frameworks of general application relevant to this study. It also provides a broad overview of certain

changes made to the UK's legal landscape due to the UK's withdrawal from the European Union (Brexit).

Data protection and ePrivacy

UK GDPR and DPA 2018

9. This sub-section covers, in brief, aspects of UK data protection legislation of most relevance to the scope of this market study.

10. The UK GDPR is the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) (the EU GDPR)). The Data Protection Act 2018 (the DPA 2018) sets out the broader data protection framework in the UK and sits alongside the UK GDPR.

11. The ICO has published detailed guidance on the application of the UK GDPR and DPA 2018, which we do not attempt to replicate here.[6] That guidance includes an explanation of the main definitions, the fundamental data protection principles (including the lawful bases for processing personal data), individual rights, and key accountability and governance obligations.

Data protection principles

12. Controllers must be able to demonstrate compliance with the following principles under article 5 UK GDPR:

- 'lawfulness, fairness and transparency'; personal data must be processed lawfully, fairly and in a transparent manner in relation to the data subject;
- 'purpose limitation'; personal data must be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes;
- 'data minimisation'; personal data must be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed;
- 'accuracy'; personal data must be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay;

[6] Guide to the UK General Data Protection Regulation (UK GDPR), and Introduction to data protection.

- ‘storage limitation’; personal data must be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; and

- ‘integrity and confidentiality’; personal data must be processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

Lawful bases for processing

13. The processing of personal data shall be lawful only if and to the extent that at least one of the following lawful bases applies under article 6 UK GDPR:

- 'consent'; the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

- 'contract'; processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

- 'legal obligation'; processing is necessary for compliance with a legal obligation to which the controller is subject;

- 'vital interests'; processing is necessary in order to protect the vital interests of the data subject or of another natural person;

- 'public task'; processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller; and

- 'legitimate interests'; processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

14. 'Consent', 'contract' and 'legitimate interests' are the lawful bases most likely to be relevant in the context of mobile ecosystems. The ICO has published more detailed guidance on consent[7] and legitimate interests[8], while the European Data Protection Board (EDPB) has adopted final guidelines on

[7] ICO detailed guidance – consent.
[8] ICO detailed guidance – legitimate interests.

processing personal data on the basis of contract in the context of online services.[9] EDPB guidelines are no longer directly relevant to the UK regime and are not binding under the UK regime. However, they may still provide helpful guidance on certain issues.

Codes of practice

15. The ICO is required to produce various statutory codes of practice under the DPA 2018 including the Data Sharing code and the Children's code. In accordance with section 127 of the DPA 2018, the ICO must take the codes into account when considering whether a controller has complied with their data protection obligations.[10]

16. The Data Sharing code[11] is a practical guide for organisations about how to share personal data in compliance with data protection law, in particular sharing information in a fair and proportionate manner.

17. The Children's code[12] (or Age appropriate design code) is a data protection code of practice for online services, such as apps, online games, and web and social media sites, likely to be accessed by children. It contains 15 standards of age appropriate design reflecting a risk-based approach. The focus is on providing default settings which ensure that children have the best possible access to online services whilst minimising data collection and use, by default.[13]

PECR

18. The PECR sit alongside the UK GDPR and DPA 2018. They give people specific privacy rights in relation to electronic communications. The PECR implement EU Directive 2002/58/EC, also known as 'the e-privacy Directive'.[14] The ICO has published detailed guidance on the PECR and its application.[15]

19. The PECR provide specific rules on: marketing by electronic means, including marketing calls, emails, texts and faxes; storage of information (and access to information stored) in users devices, including the use of cookies and similar

---

[9] EDPB final guidelines – contract.
[10] The codes can also be used in evidence in court proceedings, and the courts must take their provisions into account wherever relevant.
[11] ICO Data Sharing code of practice.
[12] ICO Children's code.
[13] The government recently consulted on proposals to reform UK data protection laws, see Data: a new direction (September 2021). The CMA has submitted a response to the consultation.
[14] The EU is in the process of replacing the current e-privacy law with a new e-privacy Regulation (ePR), to sit alongside the EU version of the GDPR. However, the ePR will not automatically form part of UK law, or sit alongside the UK GDPR, as the UK has left the EU.
[15] ICO Guidance to PECR.

technologies; keeping communications services secure; and customer privacy as regards traffic and location data, itemised billing, line identification, and directory listings.

20. Due to the prevalence of cookies and similar technologies in mobile ecosystems, the main relevance of the PECR to this study is the requirement that they specify the basic rules as to how these technologies can be used.

21. Regulation 6 of the PECR says that storage of information (or access to information stored) is prohibited unless the subscriber or user is provided with clear and comprehensive information about the purposes of that storage or access, and has given their consent. This consent must be of the UK GDPR standard.[16] This applies to anyone who undertakes these activities, by any method. It covers cookies as well as similar technologies – ie any technique that results in this storage or access.

22. For example, this means that where a cookie is not essential to provide the service, an organisation must:

- tell users the cookies are there;
- explain what the cookies are doing and why; and
- get the user's consent to store a cookie on their device.

23. In addition to its general guidance on the PECR, the ICO has produced detailed guidance on the use of cookies and similar technologies.[17]

Joint statement between the CMA and the ICO

24. The CMA and the ICO have recently published a joint statement (the Joint Statement) that sets out their shared views on the relationship between competition and data protection in the digital economy.[18] The statement sets out:

- the important role that data, including personal data, plays within the digital economy;
- the strong synergies that exist between the aims of competition and data protection;

[16] ICO Guide to the GDPR – Lawful Basis for Processing: Consent
[17] ICO guidance on the use of cookies and similar technologies.
[18] Competition and data protection in digital markets joint statement (May 2021).

- the ways that the two regulators will work collaboratively together to overcome any perceived tensions between their objectives; and

- practical examples of how the two organisations are already working together to deliver positive outcomes for consumers.

25. Of particular importance in the Joint Statement is the acknowledgement of the risk that data protection law could, in certain circumstances, be interpreted by large integrated digital businesses in a way that could lead to negative outcomes in respect of competition (for example, by unduly favouring large, integrated platforms over smaller, non-integrated suppliers).[19] At the same time, some forms of data related interventions that seek to improve competition (as well as consumer choice and control) could pose data protection and privacy risks if not carefully designed.

26. The Joint Statement provides clarification that data sharing between unconnected businesses and internal data sharing within large, integrated businesses must comply with the same data protection principles, requirements and objectives; and that neither competition nor data protection regulation allows for a 'rule of thumb' approach, where intra-group transfers of personal data are permitted while extra-group transfers are not.

Competition law

27. Below we provide a brief description of the enforcement of the prohibitions against agreements that restrict competition and the abuse of a dominant position; the review of mergers; and the market investigation regime.

28. The UK has an established set of rules to govern how the competitive process should operate to promote the economic benefits that competition between different businesses can bring for consumers, businesses, and markets. These are set out in the Competition Act 1998 (CA98) and the Enterprise Act 2002 (EA02). Public enforcement of UK competition law is the responsibility of the CMA and various 'concurrent' regulators having authority for antitrust enforcement in specific sectors of the economy alongside the CMA.[20]

---

[19] Such risks could arise, for example, from an interpretation of data protection law in which transfers of personal data between different businesses owned by a single corporate entity, such as a large platform company, are in principle viewed as acceptable from a privacy perspective. While transfers of personal data between independently-owned businesses are not, even if these businesses are functionally equivalent to those of the platform and the data is processed on the same basis and according to the same standards. For further detail see paragraphs 76 to 83 of the Joint Statement.

[20] For simplicity, this Appendix refers only to the CMA as the UK enforcer of competition, but this should be taken to include the concurrent regulators, as appropriate.

Enforcement (antitrust)

29. Competition law protects businesses and consumers against anti-competitive agreements or behaviours. The enforcement of this body of law is sometimes described as antitrust, with enforcement and the imposition of penalties and remedies where businesses are found to have infringed the law, having an important role to deter anti-competitive behaviour.

30. Chapter I of the CA98 prohibits, in certain circumstances, agreements and concerted conduct which have the purpose or effect of preventing, restricting or distorting competition in the UK. While Chapter II of the CA98 prohibits conduct which constitutes an abuse of a dominant position affecting trade within the UK.

31. More information on the laws on anti-competitive behaviour is available in the quick guide 'Competing Fairly' (OFT447)[21] and in the more detailed guidance on Agreements and Concerted Practices (OFT401)[22] and Abuse of a dominant position (OFT402).[23]

32. Where anti-competitive behaviour may affect trade between EU member states, it is also prohibited by Articles 101 and 102 of the Treaty on the Functioning of the European Union (TFEU). These prohibitions, which are effectively the same as those contained within Chapters I and II CA98, are enforced by the European Commission. Although Articles 101 and 102 are no longer of ongoing application in the UK following Brexit, decisions under those provisions adopted by the European Commission before 31 December 2020 remain binding on and in the UK.[24]

33. The European Commission has found a number infringements (and continues to bring cases) concerning digital platforms where the key issues identified concern dominant platforms shielding themselves from competition through anti-competitive restrictions in contracts, and/or leveraging their market power into related markets through the tying of particular goods/services. Of particular relevance to this study are:

    - **AT.39740 - Google Search (Shopping)**: in June 2017, the European Commission imposed a fine of €2.42bn on Google for giving favourable

[21] Competing fairly and the application of competition law: OFT447 - GOV.UK (www.gov.uk).
[22] Agreements and concerted practices: OFT401 - GOV.UK (www.gov.uk).
[23] Abuse of a dominant position: OFT402 - GOV.UK (www.gov.uk).
[24] In accordance with the Agreement on the Withdrawal of the United Kingdom of Great Britain and Northern Ireland from the European Union and the European Atomic Energy Community (the Withdrawal Agreement) Decisions adopted after 31 December 2020 remain binding where they relate to the limited number of cases over which the European Commission retains 'continued competence' under the Withdrawal Agreement.

treatment to its comparison shopping service in its search results.[25] According to the European Commission, this practice had resulted in increased traffic to Google's comparison shopping service, to the detriment of competing comparison shopping services that would have otherwise benefited from this traffic. The European Commission held that Google had abused its dominant position by (i) leveraging its dominant position on the markets for general search to the markets for comparison shopping services; and (ii) protecting its dominant position on the general search markets. In November 2021, the General Court of the European Court of Justice confirmed in principal part the European Commission's decision, confirming in particular that 'self-preferencing' can (for now) be considered a potential abuse by an undertaking deemed to be dominant.[26]

- **AT.40099 - Google Android**: in July 2018, the European Commission fined Google €4.34 billion in relation to conduct concerning certain conditions in Google's agreements associated with the use of Android, and certain proprietary apps and services.[27] In particular, the Commission concluded that Google:

  - required manufacturers to pre-install the Google Search app and browser app (Chrome), as a condition for licensing Google's app store (the Play Store);

  - made payments to certain large manufacturers and mobile network operators on condition that they exclusively pre-installed the Google Search app on their devices; and

  - prevented manufacturers wishing to pre-install Google apps from selling even a single smart mobile device running on Android forks (ie, alternative versions of Android that were not approved by Google).[28]

- **AT.40411 - Google Search (AdSense)**: in March 2019, the European Commission announced its decision to fine Google €1.49 billion for breaching Article 102 TFEU, concluding that Google had abused its dominant position in the online search advertising intermediation market by imposing a number of restrictive clauses in contracts with third-party

---

[25] European Commission decision of 27.06.2017 - Case AT.39740 - Google Search (Shopping)
[26] Google and Alphabet v Commission (Google Shopping) - Case T-612/17 - GC Judgment. It is not yet clear whether Google and Alphabet will appeal the General Court's decision.
[27] European Commission decision of 18.07.2018 - Case AT.40099 - Google Android
[28] Google and Alphabet have appealed the European Commission's decision to the General Court (Case T-604/18 – *Google and Alphabet v Commission*).

websites which prevented Google's rivals from placing their search adverts on these websites.[29]

Merger control

34. The UK merger regime is set out in the EA02. UK merger control law does not require that a qualifying merger be notified to the CMA, but the CMA may choose to review any qualifying merger. The assessment of mergers in the UK is conducted as a two-phase process, with both anticipated and completed mergers being covered by EA02.

35. The CMA assesses whether a merger will lead to a 'substantial lessening of competition' (SLC). The CMA's Merger Assessment Guidelines provide that the CMA views competition as a process of rivalry and that a merger may give rise to an SLC where it reduces levels of rivalry between firms, to the detriment of customers.[30]

36. Under the UK's two-phase merger control regime, the CMA applies different thresholds: a 'realistic prospect' threshold for a SLC in its Phase 1 initial assessment, and a 'balance of probabilities' threshold at Phase 2 (ie, is it more likely than not that an SLC will result due to the merger). If it identifies an SLC at Phase 2, the CMA decides upon the remedies required. Such remedies may include prohibiting the merger or requiring the divestiture (sale) of parts of the business.

37. The CMA's approach to mergers is set out in guidance, 'Mergers – the CMA's jurisdiction and procedure: CMA2'[31] and 'Merger assessment guidelines:CMA129.[32] The CMA recently updated its Merger Assessment Guidelines (in March 2021) in order to, among other things, provide for a more dynamic approach to assessing mergers, to place more emphasis on non-price factors of competition (eg quality and innovation), and to make clear that uncertainty will not in itself prevent the CMA from finding a competition concern. This followed the CMA's call for views, in June 2019, on our approach to the assessment of digital mergers.[33]

38. The CMA has also benefited from the large number of expert reports and academic literature that has been produced in recent years, including 'Unlocking digital competition, the Report of the Digital Competition Expert

---

[29] European Commission decision of 20.03.2019 - Case AT.40411 - Google Search (AdSense). Google and Alphabet have appealed the European Commission's decision to the General Court (*Case T-334/19 - Google and Alphabet v Commission*).
[30] Merger Assessment Guidelines (CMA129), 2.1-2.9.
[31] Mergers: Guidance on the CMA's jurisdiction and procedure (2020 - revised guidance)
[32] Merger Assessment Guidelines (CMA129).
[33] CMA call for information: digital mergers, 3 June 2019.

Panel' (March 2019);[34] and the 'Ex-post Assessment of Merger Control Decisions in Digital Markets, Final Report', an independent review of past digital mergers published in May 2019 (the LEAR Report).[35] A theme in each of these reports is the risk of under-enforcement, particularly in relation to mergers in digital markets (including the loss of potential competition in these markets), by competition authorities such as the CMA.

39. The LEAR Report included a review of the mergers in Facebook/Instagram (cleared by the OFT in August 2012);[36] Google/Waze (cleared by the OFT in November 2013);[37] and Amazon/The Book Depository (cleared by the OFT in October 2011).[38] Other recent CMA merger assessments involving digital markets include:

- Facebook/Kustomer (2021) – relating to the supply of customer relationship management software;[39]
- viagogo/StubHub (2021) – relating to the supply of online secondary ticketing;[40]
- Amazon/Deliveroo (2020) – relating to online platforms that offer restaurant and grocery delivery services;[41]
- Taboola/Outbrain (2020) – a proposed acquisition (subsequently abandoned) involving the supply of digital advertising services (including content recommendation);[42]
- Sabre/Farelogix (2020) – relating to the supply of several software solutions which help airlines to sell flights via travel agents;[43]
- Visa/Plaid (2020) – relating to the supply of technology platforms that enable digital applications to connect with bank accounts;[44]
- Google/Looker (2020) – relating to the supply of business intelligence tools;[45] and

---

[34] Unlocking digital competition: Report from the Digital Competition Expert Panel (March 2019) (The Furman Report)
[35] LEAR Report - Ex-post Assessment of Merger Control Decisions in Digital Markets, 9 May 2019.
[36] Facebook / Instagram Inc.
[37] Motorola Mobility Holding / Waze Mobile Ltd.
[38] Amazon.com, Inc / The Book Depository International Ltd.
[39] Facebook, Inc./ Kustomer, Inc.
[40] viagogo / StubHub merger inquiry.
[41] Amazon / Deliveroo merger inquiry
[42] Taboola / Outbrain merger inquiry
[43] Sabre / Farelogix merger inquiry
[44] Visa International Service Association / Plaid Inc. merger inquiry
[45] Google LLC / Looker Data Sciences, Inc merger inquiry

- Facebook (now Meta Platforms)/Giphy (2021) – relating to the supply of display advertising and of social media.[46]

Market investigation regime

40. A longstanding feature of the UK competition regime is the ability to investigate the operation of markets as a whole, as reflected in the work of this market study. The CMA may investigate to assess if a market operates in a manner which works well for consumers, and if not, may make proposals or adopt measures (remedies) so they might be made to work better.

41. Like the process described above for mergers, there is typically a two-phase process for the CMA'. The 'Phase 1' process – the market study – is used to determine whether there is a case for a more detailed examination during the 'Phase 2' process, the Market Investigation. This is achieved through the CMA making a 'market investigation reference'. The Market Investigation seeks to determine if features of the market have an adverse effect on competition (the 'AEC test'), and if so the CMA decides what remedial action, if any, is appropriate for it using its own order making powers,[47] or for others to take following a CMA recommendation. Though markets remedies are binding on businesses, in contrast to CA98 and consumer law enforcement cases, market studies and market investigations do not involve decisions as to whether or not a party has violated the relevant provisions of competition or consumer protection law. Rather, the focus of any market investigation is upon the effects on competition of possible features of the market (whether through coordinated conduct or otherwise).

42. Like in mergers, markets remedies are conventionally classified as either structural or behavioural. Structural remedies (such as a requirement to sell or separate part of a business) are generally one-off measures that seek, in market investigations, to increase competition by altering the competitive structure of the market. Behavioural remedies are generally ongoing measures that are designed to regulate or constrain the behaviour of parties in a market and/or empower customers to make effective choices.

Consumer law

43. The following paragraphs provide a non-exhaustive description of the consumer law most directly relevant to this study. The main focus is on Part 2 of the Consumer Rights Act 2015 and the Consumer Protection from Unfair

[46] Facebook, Inc (now Meta Platforms, Inc) / Giphy, Inc merger inquiry.
[47] The CMA may also accept binding undertakings from market participants.

Trading Regulations 2008, although other consumer protection legislation may apply.

The Consumer Rights Act 2015 (CRA) – Part 2

44. Part 2 of the CRA implements the Unfair Contract Terms Directive 93/13/EEC into UK law.[48]

45. Part 2 of the CRA applies to both consumer contracts and consumer notices[49] and requires the terms in such contracts and notices to be fair and, if written, transparent (that is, they must be legible and expressed in plain, intelligible language).

46. A term in a consumer contract or consumer notice is unfair if, contrary to the requirement of good faith, it causes a significant imbalance in the parties' rights and obligations under the contract, to the detriment of the consumer (the 'fairness test').

47. The 'fairness test' starts by asking whether the wording of a term tilts the rights and responsibilities between the consumer and business too much in favour of the business. The test is applied by looking how that wording could be used. It takes into consideration what is being provided, how a term relates to other terms in the contract, and all the circumstances at the time the term was agreed.

48. Some terms may be exempt from the 'fairness test' – namely those describing the main subject matter and those setting the price – provided that they are transparent and prominent. There is also an exemption for wording that reflects mandatory legislative or regulatory provisions, for example, words that legally have to be used.

49. The CRA illustrates what 'unfairness' means by listing some types of terms that may be unfair in Schedule 2 to the CRA (the 'Grey List'). These terms are not automatically unfair, but are indicative of the types of term which may be considered potentially unfair. The Grey List is not exhaustive and so terms that do not appear on it may still be unfair.

50. Transparency, as well as being a specific requirement for written terms, is also relevant to the fairness test's consideration of 'good faith'.

---

[48] Council Directive 93/13/EEC of 5 April 1993 on unfair terms in consumer contracts.
[49] A consumer notice is wording that may not form part of a contract but which relates to the same kind of issues that would be dealt with in a contract – for instance the rights or obligations between a business and a consumer.

51. To achieve the openness required by good faith, terms should be expressed fully and clearly so consumers can make informed choices about whether or not to enter the contract. Terms that might disadvantage the consumer should be given appropriate prominence. Contracts should not contain concealed pitfalls or traps.

The Consumer Protection from Unfair Trading Regulations 2008 (SI 2008/1277) (the CPRs)

52. The CPRs implement into UK law the EU Unfair Commercial Practices Directive[50] (UCPD).

53. Broadly speaking, the CPRs prevent businesses (which it describes as 'traders') from treating consumers unfairly.

54. The CPRs apply to a wide range of commercial practices which might affect consumers. Commercial practices may include matters such as advertising, marketing, sales, supplies and after-sales services. A commercial practice is governed by the CPRs if it is directly connected with the promotion, sale or supply of 'products' – which includes goods, services or digital content[51] – to consumers. Businesses are also responsible for the commercial practices of anyone who acts on their behalf or in their name. Both the business and those acting on their behalf may be held liable for breaches of the CPRs.

55. The broad scope of the CPRs means that businesses may still have to comply even when they are not selling directly to consumers themselves or are not advertising their own products.

56. There are currently 31 practices listed in Schedule 1 to the CPRs, which because of their inherently unfair nature, are prohibited in all circumstances.

57. Regulations 3, and 5 to 7 of the CPRs, also prohibit unfair practices. To be in breach of these Regulations the business must both exhibit the conduct specified in the prohibition and the practice must have, or be likely to have, an effect on the transactional decisions of the average consumer. In summary the CPRs prohibit the following conduct, where it affects consumers decisions:

[50] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer practices in the internal market.
[51] 'Digital content' refers to data produced and supplied in digital form.

- Regulation 3 contains a general prohibition on unfair commercial practices, ie, those which contravene the requirements of professional diligence.[52]

- Regulation 5 prohibits misleading actions, which occur when a business gives consumers false information (about a wide range of things listed in the CPRs), or is deceptive in the presentation of that information even if it is factually correct.

- Regulation 6 prohibits misleading omissions, which occur when businesses fail to give consumers the information that they need to make an informed choice in relation to a product. This includes hiding such information or providing it in an unclear, unintelligible, ambiguous or untimely manner.

- Regulation 7 prohibits aggressive commercial practices. These are practices that, in the context of the particular circumstances, put unfair pressure on consumers, restricting their ability to make free or informed decisions.

58. The average consumer is generally assumed to be reasonably well informed and reasonably observant and circumspect. Average does not mean a statistically average consumer. Where a commercial practice is targeted at a particular group or it is reasonably foreseeable that a group of consumers will be particularly vulnerable to that practice, then the average consumer refers to the average member of that group.

59. The CPRs prohibit unfair practices which affect a wide range of decisions taken by consumers in relation to products before, during or after a commercial transaction (if any). This is not simply confined to a consumer's decision whether or not to purchase a particular product but could also include, for example, a consumer's decision to view a product on a website, contact a business or visit a shop, as well as a decision not to purchase a particular product or to exercise a contractual right.

What about 'free' services?

60. The overarching intention of consumer law is to protect consumer's economic interests. However, that does not necessarily mean that contracts involving non-monetary consideration will fall outside its scope entirely. Courts in various international jurisdictions have accepted that a consumer's personal

[52] This is defined as meaning the standard of special and care which a trader may reasonably be expected to exercise towards consumers which is commensurate with honest market practice or good faith in their field of activity.

data, preferences and user-generated content can have an economic value[53] and are each a valid form of consideration in return for a service.

Post-Brexit changes

61. Following the UK's exit from the European Union ('Brexit') on 31 January 2020, and the subsequent end of the 'Transition Period'[54] on 31 December 2020, a number of changes to the UK's legal landscape – including to the competition and consumer regimes – have come into force. In particular, and in order to provide a level of continuity following the end of the Transition Period, the government legislated to preserve in domestic law, as far as possible, the legal position applicable immediately before the end of the Transition Period.

Post-Brexit changes relevant to competition enforcement

62. Prior to the end of the Transition Period, section 60 of the CA98 had provided that, so far as possible, the CMA, concurrent regulators and the UK courts were to interpret the Chapter I and II prohibitions in a manner consistent with the principles of the TFEU and the decisions and principles laid down by the EU Court of Justice (CJEU) in relation to the EU competition law prohibitions (Article 101 and 102 TFEU). Regard was also to be had to any 'relevant decision or statement' of the European Commission.

63. To reflect the UK's withdrawal from the EU, the government legislated to repeal section 60 CA98 and replaced it with a new provision, section 60A CA98. Under section 60A, the default position remains that the CMA, concurrent regulators and the UK courts must act with a view to securing that there is no inconsistency between:

- the principles that they apply, and the decisions they reach, in determining a question arising under Part 1 of CA98 (which includes the Chapter I and Chapter II prohibitions) in relation to competition within the UK; and
- the principles laid down by the TFEU and the CJEU before the end of the Transition Period, and any relevant decision made by that Court before the end of the Transition Period, so far as applicable immediately before

[53] The EU Commission stated: "*personal data, consumer preferences and other user generated content have a "de facto" economic value …"* European Commission, *Commission Staff Working Document: Guidance on the implementation / application of Directive 2005/29/EC on Unfair Commercial Practices* (SWD(2016) 163 final), p 25.
[54] Provided for by Article 126 of the Withdrawal Agreement.

the end of the Transition Period in determining any corresponding question arising in EU law.

64. However, section 60A allows the CMA, concurrent regulators and the UK courts to depart from the principles of the TFEU and CJEU case law pre-dating the end of the Transition Period where they consider it 'appropriate' to do so, in light of a number of prescribed factors.[55] In addition, the CMA, concurrent regulators and the UK courts will not be required to act with a view to securing that there is no inconsistency between the principles they apply or decisions they reach and any TFEU or CJEU principles or decisions pre-dating the end of the Transition Period, where they are bound by a principle or decision of a court or tribunal in England and Wales, Scotland or Northern Ireland that requires them to act otherwise.

65. Section 60A applies to all competition enforcement actions from 31 December 2020 onwards (including any CMA or concurrent regulator investigations or UK court cases which are 'live' on that date) and, extends in such cases to facts pre-dating 31 December 2020.

66. Further details regarding the changes to the UK's competition and consumer regimes following Brexit are set out in the CMA's Guidance on the functions of the CMA after the end of the Transition Period.

Non-legislative framework(s)

67. The development of the internet and internet-enabled businesses has been enabled by effective non-legislative standard setting, as has been the case in the wider information technology space. While it is beyond the scope of this Appendix to cover this in detail, certain material matters of relevance to mobile ecosystems are described briefly below.

Tech standards and standard setting bodies

68. The **Internet Society** is a supervisory organisation comprising individuals, corporations, non-profit organisations and government agencies from the internet community. It provides the administrative home for:

- the **Internet Engineering Task Force** (IETF), a loosely self-organised group who contribute to the engineering and evolution of Internet technologies by producing relevant technical and engineering documents (including protocol standards and best current practices documents) that

[55] See Guidance on the functions of the CMA after the end of the Transition Period.

influence the way people design, use, and manage the Internet.[56] It aims to support the evolution of the internet and maintain the smooth running of the internet as a whole, by developing and maintaining the Request For Comment documents that define the open standards by which the internet is managed. These open standards are developed via rough consensus; and,

- the **Internet Architecture Board**, responsible for defining the overall architecture of the internet, and providing advice, guidance and broad direction to the IETF. It also provides oversight of:
  - the **Internet Corporation for Assigned Names and Numbers** (ICANN), primarily responsible for assigning domain names and considering the introduction of new generic top level domains; and,
  - the **Internet Assigned Numbers Authority**, operated by ICANN and is primarily responsible for assigning IP addresses.

69. The **World Wide Web Consortium** (W3C)[57] develops Web standards via its international community of Member organisations, a full-time staff, and the public. W3C's primary activity is to develop protocols and guidelines that aim to ensure long-term growth for the Web. The W3C adopts a process[58] to get to a 'W3C Recommendation' or 'standard', via workshops, activity proposals, and working groups (by which specifications and guidelines are reviewed and revised).

70. There is also a wider range of more formal standard setting organisations which adopt relevant standards, such as the International Telecommunication Union, International Electrotechnical Commission, and the Institute of Electrical and Electronics Engineers.

Potential changes to the legal or regulatory landscape

71. In addition to the existing legal regime, there are various plans for new legislation in the UK relating to digital markets and online content. While these new rules remain at a reasonably early stage and are yet to be scrutinised by Parliament, we have summarised below those that are most relevant to the issues under consideration in the market study.

---

[56] RFC 3935, 4677 etc.
[57] http://www.w3.org.
[58] W3C Process.

The DMU and the new pro-competitive regime for digital markets

72. As set out in Chapter 8 of the main report, the government is proposing to establish a new pro-competition statutory regime which will proactively shape the behaviour of digital firms with significant and far-reaching market power, by making clear how they are expected to behave. The regime is intended to boost competition and innovation by tackling the sources of existing and future strategic market power. The regime will be implemented and enforced by a dedicated body, the DMU, whose core purpose is presently proposed to be 'to promote competition by addressing both the sources of market power and the economic harms that result from the exercise of market power.'[59]

73. The DMU was launched earlier this year in 'shadow form' (ie non-statutory form) within the CMA, awaiting statutory powers and objectives. The government launched a consultation in August 2021 setting out its proposals for the new regime.[60] The government's consultation followed and built on recommendations by the Digital Competition Expert Panel, and advice from the Digital Markets Taskforce. The CMA published its response to the government's consultation on 29 September 2021, noting its strong support for the government's proposals.[61]

74. The DMU's proposed powers and responsibilities (for example, regarding Strategic Market Status designations; codes of conduct; and pro-competitive interventions) are explained in detail in Chapter 8 of the main report.

Online Safety Bill

75. The UK government's draft Online Safety Bill (OSB)[62] was published in May 2021. The OSB aims to protect the UK population from illegal or harmful online content, by making digital platform operators (Regulated Providers) responsible for swiftly removing such content.

76. The OSB will apply to 'regulated services', which are either user-to-user services, such as those internet services that host user-generated content or facilitate online interaction between users, or search services (ie, search engines).

77. The companies affected will be those providing the above services that have a significant number of UK users, where the UK forms a target market for the service or where there is a material risk of significant harm to individuals in the

---

[59] A new pro-competition regime for digital markets – Consultation document (August 2021).
[60] The consultation closed on 1 October 2021, and the feedback to it is currently being considered by the Government.
[61] CMA response to the government's consultation 'A new pro-competition regime for digital markets.
[62] Draft Online Safety Bill.

UK using the service. Given the wide scope of the OSB, this will include certain mobile phone apps. The Bill will impose a duty of care on the affected companies to take proportionate measures to minimise the spread of illegal online content or activities and ensure that users are not exposed to harmful content.

78. Compliance with the OSB will be overseen by Ofcom, who will classify the online companies as Category 1, 2A or 2B services (based on thresholds set by the Secretary of State), to help determine the obligations they are under. Category 1 will be used for those services with greater users and functionality, and thereby subject to additional duties. Ofcom will also have a range of sanctions, including the ability to impose fines of up to the greater of £18 million or 10% of a Regulated Provider's qualifying worldwide revenue.

The Product Security and Telecommunications Infrastructure Bill

79. The UK government introduced the Product Security and Telecommunications Infrastructure Bill (the PSTI Bill) in November 2021.[63] The PSTI Bill supports the rollout of future-proof, gigabit-capable broadband and 5G networks, and better protects citizens, networks and infrastructure against the harms enabled through insecure consumer connectable products.

80. The bill has two main parts, covering:

- Product Security measures (Part 1); and
- Telecommunications Infrastructure measures (Part 2).

81. The Product Security measures, which may be of most relevance to the topics under consideration in this market study, are designed to:

- ensure that consumer connectable products, such as smartphones, smart TVs, internet-connectable cameras and speakers, are more secure against cyber attacks, protecting individual privacy and security;
- require manufacturers, importers and distributors to comply with new security requirements relating to consumer connectable products; and
- create an enforcement regime with civil and criminal sanctions aimed at preventing insecure products being made available on the UK market.

82. The product security measures follow extensive engagement with the National Cyber Security Centre, tech and retail industry stakeholders, consumer

[63] Product Security and Telecommunications Infrastructure Bill - Parliamentary Bills - UK Parliament.

groups and academia. The government also held a consultation on this topic in 2019,[64] and issued a call for views last year[65] (the response to which was published in April 2021).[66]

[64] Consultation on regulatory proposals on consumer IoT security - GOV.UK (www.gov.uk).
[65] Policy paper overview: Proposals for regulating consumer smart product cyber security - call for views - GOV.UK (www.gov.uk).
[66] Regulating consumer smart product cyber security - government response - GOV.UK (www.gov.uk).