The UK's Approach to Regulation of Digital Platforms

Lorna Woods

Abstract: This chapter provides an overview of three main strands of regulation in the UK that would affect the regulation of digital platforms in general and social media in particular: data protection; competition; and the online harms agenda. In doing so, it considers the extent to which existing powers have been used and the extent to which new regimes have been proposed or are required. All the regimes have a regulator and, despite potential overlap and tensions between regimes, a number of commonalities exist between them, notably the focus on the impact of design choices, and risk-based approaches to the applicability of the regimes. A further similarity is the question of whether the regulators have adequate powers and resources. A final theme is the response, particularly of large companies, to enforcement of regulation.

Keywords: data protection – competition – consumer protection – online harms – online safety – targeted advertising – age appropriate design code – digital markets unit

Chapter 1. Introduction

The last decade has seen the beginning of attempts to regulate online platforms, a trend which has picked up pace since the Cambridge Analytica scandal and other *causes célèbres*. This contribution outlines policy developments in the UK across three relevant policy fields: data protection; competition and consumer protection; and online harms. In so doing, it considers both the re-purposing of existing powers and the proposal of entirely new regimes. This paper will identify how existing regimes have been used; what new measures are proposed and where the legislative process currently sits in a policy environment dominated by Brexit and COVID-19.

Chapter 2. Data Protection

Although data protection has received a much higher profile[1] with the introduction of the General Data Protection Regulation (GDPR)[2] (implemented in the UK by the Data Protection Act 2018 (DPA18)), the fundamental principles of data protection have not changed radically from the previous regime (Data Protection Act 1998 (DPA98), implementing the Data Protection Directive[3]). It is enforced by the Information Commissioners Office (ICO), an independent regulatory authority.[4] While much of the ICO's enforcement activity has focused on inadequate security,[5] but beyond this there are three interconnected areas affecting online platforms: the Cambridge Analytica investigation (including the investigation regarding political campaigns); the investigation into the online advertising sector; and the Age Appropriate Design Code.

Chapter 3. Cambridge Analytica and the Use of Data for Political Purposes

The ICO commenced an investigation into the use of data analytics in political campaigning in the light of concerns about "invisible processing" and micro-targeting of political adverts[6] triggered by the Cambridge Analytica scandal. Cambridge Analytica, a political consultancy firm, combined data obtained from a quiz app with data obtained through Facebook's Graph API and other data sources to profile users in furtherance of its clients' objectives. Users of the quiz app were unaware of the data collection and use. The ICO investigation covered social media platforms, but

1 C. Sellars, "GDPR: one year on - ICO pulls back the curtain on the impact of the new regime", (2019) 25 *CTLR* 172, pp. 172 and 173.

2 Regulation 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC [2016] OJ L119/1.

3 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L281/31.

4 The relationship with the Department of Digital Culture Media and Sport is set out in a management agreement between the ICO and DCMS, https://ico.org.uk/media/about-the-ico/documents/2259800/management-agreement-2018-2021.pdf.

5 A. Bevitt and A. Collins, "UK Enforcement: Five focus areas", (2020) 20 *Privacy and Data Protection* 10.

6 Select Committee on Digital Culture Media and Sport, *Disinformation and 'fake news': Final Report*, 18 February 2019, https://publications.parliament.uk/pa/cm201719/cmselect/cmcumeds/1791/179102.htm.

also data brokers, analytics firms, political parties and campaign groups. Its report concluded that there were risks in relation to the processing of personal data by many political parties. Particular concerns included the purchasing of marketing lists and lifestyle information from data brokers without sufficient due diligence; a lack of fair processing; and the use of third party data analytics companies, with insufficient checks around consent.[7] Formal warnings were issued to 11 political parties, and a number of fines imposed (including one of £500,000 on Facebook[8] – the maximum allowable under the DPA98 which applied at the time the incidents occurred). The interim report[9] also contained assessment notices to the three main credit reference agencies – Experian, Equifax and Call Credit.[10] Experian's response was subsequently found to be insufficient, and the ICO issued an enforcement notice (but not yet a fine).[11] The investigation concluded that there had not been significant interference in

7 For the interplay between data protection rules and rules pertaining to electoral advertising, see B. Shiner, "Big data, small law: how gaps in regulation are affecting political campaigning methods and the need for fundamental reform", (2019) *Public Law* 362; concerns about micro-targeting have also been expressed at EU level: C. Wenn, "Can data protection solve the problem of microtargeting, manipulation of internet users and fake news?", (2018) 29 *Ent. LR* 216.

8 ICO, Press Release, ICO issues maximum £500,000 fine to Facebook for failing to protect users' personal information, https://ico.org.uk/facebook-fine-20181025#.

9 ICO, *Democracy disrupted? Personal information and political influence*, 11 July 2018, https://ico.org.uk/media/action-weve-taken/2259369/democracy-disrupted-110718.pdf; ICO, Investigation into the use of data analytics in political campaigns: Investigation update, 11 July 2018, https://ico.org.uk/media/action-weve-taken/2259371/investigation-into-data-analytics-for-political-purposes-update.pdf; and ICO *Investigation into the use of data analytics in political campaigns: A Report to Parliament*, 6 November 2018, https://ico.org.uk/media/action-weve-taken/2260271/investigation-into-the-use-of-data-analytics-in-political-campaigns-final-20181105.pdf.

10 See report of the investigation: ICO, Investigation into data protection compliance in the direct marketing data broking sector, October 2020, https://ico.org.uk/media/action-weve-taken/2618470/investigation-into-data-protection-compliance-in-the-direct-marketing-data-broking-sector.pdf. Regulatory action (but not an audit) was taken in relation to a data broker, Emma's Diary: ICO, Emma's Diary fined £140,000 for selling personal information for political campaigning, 9 August, 2018, Press Release: https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/08/emma-s-diary-fined-140-000-for-selling-personal-information-for-political-campaigning/.

11 ICO, ICO takes enforcement action against Experian after data broking investigation, 27 October 2020, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/10/ico-takes-enforcement-action-against-experian-after-data-broking-investigation/.

elections[12] (seemingly some claims of influence by Cambridge Analytica may have been unfounded). Given the general poor compliance with basic principles of data protection law in this area, however, the ICO has published guidance to political parties on the use of personal data in political campaigns.[13]

Despite what might seem unremarkable conclusions, the investigation is significant not just for the interpretation of the substantive obligations but also for the ICO's use of its enforcement powers which had been extended by the DPA18 (e.g., compulsory audit under Article 58(1)(b) GDPR). The wide territorial reach of the GDPR is illustrated by the investigation of Aggregate IQ (AIQ), a Canadian analytics firm linked to Cambridge Analytica. The ICO served an enforcement notice under section 149 DPA18,[14] its first notice under the GDPR/DPA18 regime, requiring AIQ to cease processing the personal data of UK and EU citizens, processing that was in violation of Articles 5, 6 and 14 GDPR. It was also the first time the ICO, relying on Article 3(2)(b) GDPR, had attempted to enforce against an entity outside the jurisdiction. It determined that the GDPR rather than just the Directive was relevant because, although the data were collected before the entry into force of the GDPR, AIQ continued to hold (and therefore process) the data afterwards.

The possibility of such extraterritoriality had been recognised as the GDPR came into force[15]. The election investigation showed that extraterritoriality might also operate when the relevant parties' locations were reversed. The ICO served an enforcement notice on SCL Elections Ltd (a UK company) to compel it to deal properly with a data subject access request from an American, Professor Carroll. SCL responded that non-UK citizens had no rights under the GDPR, a view the ICO did not share. It took the position that SCL was based in the UK and therefore subject to the law of that jurisdiction. The question has not yet been judicially considered.

12 ICO, Letter to Digital, Culture and Media and Sport Select Committee, 2 October 2020, https://ico.org.uk/media/action-weve-taken/2618383/20201002_ico-o-ed-l-rtl-0181_to-julian-knight-mp.pdf.

13 ICO, Guidance for the use of personal data in political campaigning, https://ico.org.uk/for-organisations/guidance-for-the-use-of-personal-data-in-political-campaigning/.

14 https://ico.org.uk/media/2259362/r-letter-ico-to-aiq-060718.pdf.

15 See e.g. K Hon, "GDPR's extra-territoriality means trouble for cloud computing", (2016) 140(Apr) *Privacy Laws and Business International Newsletter* 25.

In addition to the ICO enforcement notice, AIQ (along with other companies – for example Facebook) were subject to investigation in other jurisdictions. So, this case also illustrates the importance of international regulatory cooperation.

In this enforcement action, the ICO also used its criminal enforcement powers under s47(1) DPA98 against SCL, which had chosen to ignore the enforcement notice the ICO had issued in relation to Professor Carroll.[16] This tough approach to enforcement was reinforced by the ICO referring SCL, as it had become insolvent, to the Insolvency Service, which in turn disqualified the directors of the company from acting as such for a period of seven years.[17] Suggesting that it would not be easy for those behind a company to avoid regulation by establishing new companies, the ICO stated that it would "monitor closely any successor companies using our powers to audit and inspect".[18]

Another theme relating to this investigation concerns the challenges to the ICO's decisions. Facebook challenged its fine, alleging procedural unfairness, showing that decision-making processes are important and may be a point of dispute especially where penalties are significant. The parties settled the action, with Facebook agreeing to pay the fine but, significantly, making no admission of liability as to the basis on which the fine was levied (though it had carried out an app audit[19] and changed its

16 ICO, SCL Elections prosecuted for failing to comply with enforcement notice, (January 2019), https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/01/scl-elections-prosecuted-for-failing-to-comply-with-enforcement-notice/.

17 The Insolvency Service investigation determined that "he caused or permitted SCL Elections Ltd or associated companies to market themselves as offering potentially unethical services to prospective clients; demonstrating a lack of commercial probity": The Insolvency Service, Press Release: 7-year disqualification for Cambridge Analytica boss, 24 September 2020, https://www.gov.uk/government/news/7-year-disqualification-for-cambridge-analytica-boss.

18 ICO, ICO statement: investigation into data analytics for political purposes, 2 May 2018, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2018/05/ico-statement-investigation-into-data-analytics-for-political-purposes/.

19 Facebook, An Update on Our App Investigation and Audit, 14 May 2018, https://about.fb.com/news/2018/05/update-on-app-audit/; Facebook, An Update on Our App Developer Investigation, 20 September 2019, https://about.fb.com/news/2019/09/an-update-on-our-app-developer-investigation/; Facebook Taking Legal Action Against Those Who Abuse Our Platform, 27 August 2020, https://about.fb.com/news/2020/08/taking-legal-action-against-those-who-abuse-our-platform/.

process regarding access to the API).[20] Facebook is not alone in turning to litigation, and the substance of the ICO's reasoning has been challenged as well as its processes. Leave.EU challenged[21] a fine imposed (under the Privacy and Electronic Communications Regulations[22] (PECR)) for including marketing materials in communications with Leave.EU's subscribers. It lost at first instance and was unsuccessful on appeal.[23] It has announced its intention to appeal again. Appeals by the Liberal Democrats and UKIP were dismissed at first instance.[24] Experian also plans to challenge the ICO's interpretation of the GDPR.[25]

Chapter 4. Online Advertising

The ICO cited web and cross-device tracking as one of its three regulatory priority areas in its Technology Strategy 2018-2021. Advertising and the use of data is a broad topic, but 'adtech' and real-time bidding (RTB) systems are central. Adtech is the umbrella term for the range of software and tools used to target, deliver, and analyse their digital advertising. RTB is a real-time automated digital auction process that allows advertisers to bid for online ad space from publishers, with the highest bid usually winning. Significantly, the ads are personalised; to make the assessment as to whether or how to bid, data about the person viewing the page/app must be shared through the RTB system. This brings data protection rules into play.

20 ICO, Statement on an agreement reached between Facebook and the ICO, 30 October 2019, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2019/10/statement-on-an-agreement-reached-between-facebook-and-the-ico/#.

21 A case challenging another fine for using an insurance company's mailing list to send out political material was withdrawn.

22 The Privacy and Electronic Communications (EC Directive) Regulations 2003 (SI 2003/2426), implementing the e-Privacy Directive (Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector [2002] OJ L201/37).

23 *Leave.EU and Eldon v Information Commissioner* [2021] UKUT 26 (AAC).

24 ICO, Letter to the Chair of DCMS Select Committee, 2 October, 2020, https://ico.org.uk/media/action-weve-taken/2618383/20201002_ico-o-ed-l-rtl-0181_to-julian-knight-mp.pdf.

25 Experian, Response to ICO Enforcement Notice in relation to UK marketing services, 27 October 2020, https://www.experianplc.com/media/news/2020/response-to-ico-enforcement-notice-in-relation-to-uk-marketing-services/.

The ICO announced an investigation into adtech because of its complexity and scale, the risks posed to the rights and freedoms of individuals, as well as concerns expressed by some actors about the use of the technology. The ICO released an interim report[26] identifying a number of issues of concern. Risks were found to arise from profiling within the meaning of Article 4(4) GDPR and automated decision-making; large-scale processing including of special categories of data; the use of new/innovative technologies; combining and matching data from multiple sources; geolocation tracking; the tracking of behaviour; and the fact the processing was effectively invisible (as also found in the political advertising investigation). In particular, the ICO highlighted transparency and consent to processing; while some actors sought to rely on 'legitimate interests', the ICO noted that the circumstances in which this basis for processing would be available would be limited. In general, the scale of both the creation of data and the sharing of those data was assessed as disproportionate, intrusive and unfair – especially given that data subjects were unaware that this is happening. Further, the sharing of data through the supply chain, which relied on contractual arrangements (especially standard terms and conditions), was viewed as problematic, particularly given the type of personal data shared and the number of intermediaries involved.

The interim report gave the industry six months to respond to the issues raised.[27] Despite some changes[28], the ICO subsequently commented:

"while many organisations are on board with the changes that need making, some appear to have their heads firmly in the sand".[29]

Its activities on this project were suspended as a result of the pandemic; it was only in January 2021 that the ICO announced that its investigation was to re-start.[30] Nonetheless, there has been some concern amongst civil society actors as to the rate of progress; against this background there is

26 ICO Update report into adtech and real time bidding, 29 June 2019, https://ico.org.uk/media/about-the-ico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf.

27 S. McDougall, Blog: Adtech - the reform of real time bidding has started and will continue, 17 January 2020, https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-the-reform-of-real-time-bidding-has-started/.

28 See e.g. M. Dunphy-Moriel and S. Dittel, "A real-time bid to restore trust in online advertising: DMA's seven-step ad tech and other industry initiatives" (2020) 31 *Ent. LR* 233.

29 McDougall (n. 27).

30 ICO, Press Release: Adtech investigation resumes, 22nd January 2021, https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2021/01/adtech-investigation-resumes/.

increasing strategic litigation (including collective actions).[31] The role of representative bodies here could be significant, given the asymmetries of information and resources between individual data subjects and global businesses. The Government has, however, decided not to implement Article 80(2) GDPR.

Chapter 5. Age Appropriate Design Code

The requirement for an Age Appropriate Design Code (AADC) derives from section 123 DPA18. There were concerns that a focus on the age at which children could consent, as found in the GDPR, was insufficient to tackle problems arising from the ways platforms are designed and which do not take the various levels of children's understanding into account. The AADC aimed at ensuring that those companies which provided services to children provided services that were appropriate to the children's respective developmental stages. The inclusion of this obligation was a significant step in recognising the impact of design choices in this context.

Section 123 specifies that the Information Commissioner must prepare a code of practice on standards of age appropriate design of "relevant information society services"[32] which are likely to be accessed by children - not just those which actively target children. The draft AADC was subject to Parliamentary approval.[33] 'Age appropriate' means that the services should be designed to be appropriate for children bearing in mind their developmental stage – so that design issues will be different depending on the age group served. Note that there are no requirements as to specific technology; by contrast, the Digital Economy Act 2017, Part 3 dealing with children's access to online pornography specified age verification technology for all age groups (though these provisions were not brought into force). The DPA18 nonetheless specified a minimum range of issues

31 K. Brimstead, "All I want for Christmas is not to be sued (by you and you and you...)!" (2020) 21 *Privacy and Data Protection* 6 provides an overview of procedure; *Lloyd v Google* [2019] EWCA Civ 1599 deals with the conditions for determining whether there is a class; the Supreme Court has heard an appeal but at the time of writing the judgment had not been handed down; *CMO v TikTok* is at an early stage, progress depending on the outcome of *Lloyd*; *Rumbul* v *Oracle and Sales Force* is also at a preliminary stage.

32 Defined s 123(7) DPA 18.

33 Section 125(3) and (4) of the DPA18.

to be considered. While many of these relate to rights and requirements found in the GDPR, some might be seen as going beyond that.

The AADC incorporates the principle that the best interests of the child should be a primary consideration in all actions concerning children; in this it borrows from the approach found in the UN Convention on the Rights of the Child (UNCRC). Following the UNCRC, a child is anyone under the age of 18. The AADC sets out 15 principles of age appropriate design, reflecting the concerns identified in section 123. In addition to the focus on the best interests of the child, they are: the need to carry out data impact assessments; that approaches adopted are age appropriate; transparency requirements; children's personal data should not be used in ways detrimental to their well-being; up-hold the services policies and standards; high privacy settings should be the default position; data minimisation; children's data should not be disclosed without a compelling reason; geolocation should be switched off by default; the child should be given age appropriate information about the existence of any parental controls; consent to profiling should be opt-in rather than opt-out and only allowed when appropriate measures are in place to protect children from any harmful effects; nudge techniques should not be used to get children to turn off protections; effective tools to be provided in connected toys; and prominent and accessible tools should be provided for children to exercise their rights. These are not technical design requirements but are a set of technology-neutral design principles; as with the DPA18, the AADC does not mandate any particular solutions. Assessment and mitigation of risk falls to service providers.[34] It remains to be seen how these requirements will be implemented by the ICO. While the AADC is now in force, the ICO allowed a 12-month transitional period, starting on 2 September 2020, to allow business time to prepare to comply with these obligations.

The AADC was not required by the GDPR and could be seen as a domestic experiment; other countries are, however, considering design codes. The Irish Data Protection Commissioner (DPC), for example, published draft "Fundamentals for a child oriented approach to data processing" in 2020. While these 'fundamentals' are not the same as the AADC, there is some consistency between the two, for example as regards the emphasis on data protection impact assessments, approach to profiling, data minimisation, geolocation and sharing of data.

34 For discussion of some initial concerns see e.g. R. Jay, "The Age Appropriate Design Code", (2020) 21 *Privacy and Data Protection* 3.

Chapter 6. Competition and Markets Authority

The Competition and Markets Authority (CMA) is an independent non-Ministerial government department dealing with competition enforcement and consumer protection. It will be granted further powers in relation to digital markets as envisaged in a number of reviews and reports on digital markets.[35] The Furman Report recommended the creation of a Digital Markets Unit (DMU) and the Government established the Digital Markets Taskforce (the "Taskforce"), led by the CMA, to make recommendations on the establishment of a regulatory framework for digital markets.[36] The CMA will also be expected to collaborate with the other regulators with competence in the digital sectors: Ofcom, the ICO and the Financial Conduct Authority (FCA). Together they established the Digital Regulators Cooperation Forum (DRCF).[37] It should be noted that while these regulators may have the most involvement with digital markets, they are not the only regulators those markets may touch. DRCF acknowledges this, as well as the likely need for engagement internationally.

Chapter 7. Competition Policy

The CMA has responsibility under the Competition Act 1998 for enforcing the prohibition on agreements and conduct which prevent, restrict or distort competition (Chapter 1 prohibition), and conduct which constitutes an abuse of a dominant position (Chapter 2 prohibition). The CMA has the power to impose fines and, in relation to cartels, criminal sanctions may be available. The Enterprise Act 2002 (EA02) introduced

35 Report of the Digital Competition Expert Panel, Unlocking Digital Competition, March 2019 (Furman Report); Lear, Ex-post Assessment of Merger Control Decisions in Digital Markets: Prepared for the Competition and Markets Authority, 9 May 2019 (Lear Report).

36 Digital Markets Taskforce Terms of Reference: https://www.gov.uk/government/publications/digital-markets-taskforce-terms-of-reference/digital-markets-taskforce-terms-of-reference–3.

37 CMA, Ofcom, ICO, Digital Regulation Cooperation Forum Launch Document, 1 July 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/896827/Digital_Regulation_Cooperation_Forum.pdf.

market studies[38] and market investigations to the CMA toolbox. The CMA also has responsibility for reviewing mergers under the EA02.

Following the Furman Report's recommendation that there be a market study into the digital advertising market,[39] the CMA investigated three broad heads of harm: the impact on consumers of online platforms' market power; the ability of consumers to control how data about them is used and collected by online platforms; and distortion in the digital advertising market caused by any market power held by platforms. The CMA concluded that "concerns we have identified in these markets are so wide ranging and self-reinforcing that our existing powers are not sufficient to address them".[40] The Government envisaged the recommendations from the market study would be taken forward through the establishment of the DMU.[41]

The Taskforce's advice[42] envisaged that the DMU be established within the CMA. It will operate a new regime applying to certain digital businesses designated as having "strategic market status" (SMS). The test for SMS is where a company has a "substantial, entrenched market power in at least one digital activity, providing the firm with a strategic position". SMS status would apply to the entire group of which the relevant company formed part. These businesses would be subject to an *ex ante* regime with three main elements. The first is a binding statutory code of conduct (with financial penalties of up to 10% of worldwide turnover for breach of the code). Secondly, the DMU would initiate proactive interventions

38 Market studies examine why a particular market may not be working well. The range of possible outcomes includes recommendations to government or initiation of a market investigation.

39 An investigation was also recommended by the Cairncross Review into Sustainable Journalism, 12 February 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/779882/021919_DCMS_Cairncross_Review_.pdf as well as the House of Lords Report, Regulating in a Digital World (HL Paper 299), 9 March 2019, available: https://publications.parliament.uk/pa/ld201719/ldselect/ldcomuni/299/299.pdf.

40 CMA, *Online platforms and digital advertising Market study final report,* 1 July 2020, p. 5, https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf.

41 BEIS and DCMS, Government Response to the CMA's market study into online platforms and digital advertising, November 2020, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/939008/government-response-to-cma-study.pdf.

42 CMA, *A new pro-competition regime for digital markets: Advice of the Digital Markets Taskforce,* December 2020 (CMA 135), https://www.gov.uk/cma-cases/digital-markets-taskforce.

targeted at SMS firms, including interventions relating to personal data mobility, interoperability and access to data so as to promote competition and innovation. Finally, special merger rules will require SMS firms to report all transactions to the CMA; normally the UK merger regime does not require parties to notify transactions. The new regime will also impose mandatory and suspensory notification requirements for transactions that meet certain thresholds. Although the Government has committed to introducing legislation to introduce the new regime, it is unclear when there will be Parliamentary time for the bill. Nonetheless, the DMU itself was launched on a non-statutory basis to focus on operationalising and preparing for the new regime on 7 April 2021.[43]

The CMA has also reviewed its Merger Assessment Guidelines[44] to reflect its recent decisional practice under the Competition Act which takes account of a broader context and the risk of consumer harm in assessing whether the threshold for intervention is met. Its approach to the 'share of supply' test,[45] allowed it to intervene in deals involving targets with very low (or even no) turnover, for example when technology rights are involved, and has been approved by the Competition Appeal Tribunal (CAT).[46] In all this, the CMA seems to take a comparatively interventionist stance,[47] and has challenged some deals that have been permitted by other competition authorities around the world.

The CMA's expansive use of its powers has, however, been subject to legal challenge.[48] Facebook appealed against the CMA's intervention[49] in Facebook's acquisition of Giphy, arguing the intervention was irrational, disproportionate and infringed the principle of legal certainty. The CAT unanimously dismissed the application,[50] and the CMA is now carrying

43 https://www.gov.uk/government/collections/digital-markets-unit.
44 CMA, *Merger Assessment Guidelines* (CMA129), 18 March 2021, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/986475/MAGs_for_publication_2021_-.pdf.
45 S. 23(2)(b) EA02.
46 *Sabre Corporation v Competition and Markets Authority* [2021] CAT 11.
47 M. Jephcott and V. Karadakova, 'The CMA's increasingly expansionist approach to the share of supply test in UK merger control: a threshold issue", (2020) 41(9) *European Competition Law Review* 466.
48 Section 120 EA02; *Sabre* (n47) is another example.
49 It imposed an initial enforcement order (IEO) aimed at preventing pre-emptive action by the companies involved which might otherwise restrict the CMA's ability to secure remedies at the conclusion of its merger review.
50 *Facebook v CMA* [2020] CAT 23.

out a full merger inquiry.[51] Facebook, however, is pursuing the action against the CMA before the appellate courts.[52]

It should be noted that the CMA has not just applied its powers in relation to mergers. For example, it has opened an investigation into Apple's app store, in particular, the terms and conditions governing app developers' access to Apple's App Store under the Chapter II prohibition. It has similarly launched an investigation into Google's 'privacy sandbox' changes to its Chrome browser. Note that those changes introduced and potentially problematic in a competition context might be seen as a good thing from the data protection perspective.[53] The ICO and CMA have issued a joint statement,[54] but this tension highlights the importance of the DRCF as a venue for regulatory coordination and cooperation. Finally, the CMA has opened an investigation into whether Facebook has unfairly used the data gained from its advertising and single sign-on to benefit its own services, notably Facebook marketplace. It is noteworthy that the EU Commission has also launched an investigation. While the two investigations are separate, the CMA envisages working closely with the European Commission on this issue.[55]

Chapter 8. Consumer Protection

The CMA also has competence in the consumer protection field under the Enterprise Act 2002 (as amended) (EA02). It is not the only body with consumer protection powers: The Trading Standards Authority, for example, deals with misleading statements and acts as backstop regulator to the Advertising Standards Authority (ASA) in relation to advertisements not caught by the audiovisual regime. The CMA's enforcement powers

51 https://www.gov.uk/cma-cases/facebook-inc-giphy-inc-merger-inquiry.

52 *Facebook v CMA* (nyd); hearing available here: https://www.judiciary.uk/publications/facebook-inc-another-v-the-competition-and-markets-authority/.

53 This tension is discussed by D. Geradin et al, "GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech", (2021) 17 *European Competition Journal* 47.

54 CMA and ICO, *Competition and data protection in digital markets: a joint statement between the CMA and the ICO*, 19 May 2021, https://ico.org.uk/media/about-the-ico/documents/2619797/cma-ico-public-statement-20210518.pdf.

55 CMA, Press Release: CMA investigates Facebook's use of ad data, 4 June 2021, https://www.gov.uk/government/news/cma-investigates-facebook-s-use-of-ad-data.

include both civil and criminal mechanisms.[56] Part 8 EA02 constitutes the main civil enforcement regime, giving the CMA the power to apply to the court for an enforcement order in relation to any rules identified by the EA02. These orders may include 'enhanced consumer measures' which require business to take additional steps for the protection of consumers. Alternatively, the CMA may accept an undertaking from the relevant business. The CMA also has powers under the Consumer Rights Act 2015 in relation to unfair terms.[57] The UK retained after Brexit rules[58] derived from the EU Consumer Protection Co-Operation Regulation.[59]

Using its current powers, the CMA has launched a number of consumer protection investigations in the online context: fake online reviews (leading to commitments from Facebook to do more to tackle the problem in 2020 and in 2021[60]); unfair roll-over contracts in subscriptions for online gaming[61] and anti-virus software;[62] problems with nudging techniques on hotel booking sites;[63] unclear policies especially as regards data sharing on data-sites;[64] and lack of disclosure of incentivised endorsements on social media platforms. The CMA has tackled a wide range of issues: these investigations have identified issues with content, business models as well as with platform design.

As with the ICO, international collaboration is important in this sector. The CMA's work on dating platforms was part of an international project on the fairness of platforms' terms and conditions.[65] The project overall aimed at securing disclosure around the data collection and privacy terms

56 Criminal enforcement powers are found in The Consumer Protection from Unfair Trading Regulations 2008 (SI 2008/1277), https://www.legislation.gov.uk/uksi/2008/1277/contents/made.

57 The CMA's approach to these powers is described in its guidance on unfair terms: CMA, Unfair Contract Terms Guidance, 31 July 2015 (CMA37) para 6.4, https://www.gov.uk/government/publications/unfair-contract-terms-cma37.

58 The Consumer Protection (Enforcement) (Amendment etc.) Regulations 2020 (SI 2020/484), https://www.legislation.gov.uk/uksi/2020/484/made.

59 Regulation 2017/2394 Consumer Protection Co-Operation Regulation [2017] OJ L345/1.

60 https://www.gov.uk/government/news/cma-intervention-leads-to-further-facebook-action-on-fake-reviews.

61 https://www.gov.uk/cma-cases/online-console-video-gaming.

62 https://www.gov.uk/cma-cases/anti-virus-software.

63 https://www.gov.uk/cma-cases/online-hotel-booking.

64 https://www.gov.uk/cma-cases/online-dating-services.

65 CMA, Blog: Why we're banging the drum for international fairness in the digital economy, 29 June 2018, https://competitionandmarkets.blog.gov.uk/2018/06/29/why-were-banging-the-drum-for-international-fairness-in-the-digital-economy/.

of apps as well as to prevent nudging techniques being used in breach of consumer protection rules (e.g. pressure selling, scarcity claims and subscription traps).

The CMA has also worked with other UK regulators, for example the Gambling Commission, which was concerned about potentially unfair terms and practices in the online gambling sector.[66] The work on non-disclosed adverts by influencers has also fallen within the remit of the co-regulator, the ASA, which has targeted advertisers and influencers;[67] the CMA's work, by contrast, resulted in undertakings from the platforms themselves (as well as guidance to influencers[68]). The ASA's work is not limited to non-disclosure issues but extends to ensuring compliance with all advertising rules.

Nonetheless, the CMA has expressed concerns about the effectiveness of these powers, especially in the digital context, and has suggested that there be legislative reform of its consumer protection powers.[69] The CMA characterised its enforcement powers as weak; it highlighted the fact that it cannot order the cessation of practices it considers to be illegal, but must pursue businesses through the courts and even then no fines are available. It proposed bringing its consumer protection powers in line with its competition powers, so that the CMA would be able to decide whether consumer protection law has been broken; declare the fact publicly; direct businesses to bring infringements to an end; and impose fines. It also

66 https://www.gov.uk/government/news/gambling-sector-told-to-raise-its-game-after-cma-action; discussed J. Althoff, "Crackdown in the online gambling sector", (2018) 29(1) *Ent LR* 7.

67 ASA, *Influencer Ad Disclosure on Social Media - A report into Influencers' rate of compliance of ad disclosure on Instagram*, https://www.asa.org.uk/uploads/assets/dd740667-6fe0-4fa7-80de3e4598417912/Influencer-Monitoring-Report-March2021.pdf; see also ASA guidance for influencers: https://www.asa.org.uk/resource/influencers-guide.html; discussed O. Bray and V. Noto, "#Ad-vice for influencers and brands: how to comply with CAP's new influencer's guide", (2019) 30(1) *Ent. LR* 11; J. Agate et al., "Influencer advertising: the latest ASA findings" (2020) 31(1) *Ent LR* 14.

68 CMA, Guidance: Social media endorsements: being transparent with your followers, 23 January 2019, https://www.gov.uk/government/publications/social-media-endorsements-guide-for-influencers/social-media-endorsements-being-transparent-with-your-followers.

69 CMA, Letter to the Secretary of State for Business, Energy and Industrial Strategy, 21 February 2019, https://www.gov.uk/government/publications/letter-from-andrew-tyrie-to-the-secretary-of-state-for-business-energy-and-industrial-strategy/summary-of-proposals-from-andrew-tyrie-cma-chair-to-the-secretary-of-state-for-business-energy-and-industrial-strategy.

suggested that it should be able to order the cessation of practices on an interim basis. In addition to considering fines, it suggested that the CMA should be able to seek the disqualification of company directors. This is the case for competition law but few cases have resulted in disqualification orders.[70]

The Taskforce highlighted specific issues based on the CMA's experience in digital markets. It noted the problematic use of dark patterns and nudging techniques, suggesting that a more explicit duty on firms "to take reasonable and proportionate steps to reflect consumers' interests in the design of their products and services" could be a means of tackling this issue.[71] In proposing this solution, the Taskforce noted that such an approach would complement the 'fairness by design' duty suggested in the CMA's market study final report,[72] as well as the statutory duty of care proposed in the Online Harms White Paper (OHWP).[73] The Taskforce also noted the importance of stronger enforcement of the Platform to Business Regulation[74] (as retained). Again, it is unclear what the legislative timetable would be for bringing in any changes.

---

70 Sections 9A- 9E Company Directors Disqualification Act 1986; CMA, Guidance on Competition Disqualification Orders, 8 February 2019 (CMA 102), available: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/910485/CMA102_Guidance_on_Competition_Disqualification_Orders__FINAL__PDF_A-.pdf; C. Chijioke-Oforji, "Director accountability for breach of competition law: important practical lessons from the CMA's increased use of disqualification powers", (2021) 42 *European Competition Law Review* 24 and S. Caliskan 'Directors' disqualification in UK competition law: has the dog started barking?" (2020) 41 *European Competition Law Review* 509 discusses the recent use of these powers in the competition arena.

71 CMA, A new pro-competition regime for digital markets Advice of the Digital Markets Taskforce, December 2020 (CMA135), https://assets.publishing.service.gov.uk/media/5fce7567e90e07562f98286c/Digital_Taskforce_-_Advice.pdf, para 5.26.

72 CMA, Market Study into Online Platforms and Digital Advertising, 1 July 2020, available: https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf, paras 8.123-8 and Appendix Y.

73 DCMS Online Harms White Paper (CP57), 8 April 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/973939/Online_Harms_White_Paper_V2.pdf.

74 Regulation (EU) 2019/1150 on promoting fairness and transparency for business users of online intermediation services OJ [2019] L186/57.

Chapter 9. Internet Safety and Online Harms

In the Autumn of 2017, the Government published a Green Paper on Internet Safety.[75] It identified a wide range of concerns[76] but mainly envisaged self-regulation and media literacy as the tools to deal with them. Government policy underwent a rapid change. In Spring 2018, the Secretary of State announced that as part of its Digital Charter, the government would introduce laws to ensure that "the UK is the safest place in the world to be online", reflecting the words of then Prime Minister, Theresa May, at Davos in January 2018. The proposed approach was at that stage unclear; the Online Harms White Paper (OHWP) did not emerge until April 2019. Unusually for a white paper, a number of details were undecided so the OHWP also constituted a consultation on those elements. Further progress was slow. There was an interim response to the OHWP[77] before the Full Government Response (FGR)[78] was published on 15 December 2020. In the meantime, however, the UK implemented the changes to the Audiovisual Media Services Directive[79] meaning the provisions on video sharing platforms have been in force in the UK since 1 November 2020, with Ofcom, the independent communications and media regulator, as the competent body. The Government also decided not to bring into force Part 3 of the DEA, a decision which has been contentious. Following the Queen's Speech for the 2021-22 Parliamentary session, the Government published the draft Online Safety Bill (OSB) for pre-legislative scrutiny.[80]

The OHWP proposed imposing a statutory duty of care on operators within remit. While the OHWP did not specify the extent of this duty,

75 DCMS, *Internet Safety Strategy Green Paper*, 11 October 2017, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/650949/Internet_Safety_Strategy_green_paper.pdf.

76 See Annex A to the *Internet Safety Green Paper* (n. 76).

77 DCMS, Online Harms White Paper - Initial consultation response, 12 February 2020, https://www.gov.uk/government/consultations/online-harms-white-paper/public-feedback/online-harms-white-paper-initial-consultation-response.

78 DCMS, Online Harms White Paper: Full Government Response to the consultation, December 2020 (CP354), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/944310/Online_Harms_White_Paper_Full_Government_Response_to_the_consultation_CP_354_CCS001_CCS1220695430-001__V2.pdf.

79 The Audiovisual Media Services Regulations 2020 (SI 2020/1062), https://www.legislation.gov.uk/uksi/2020/1062/made.

80 Pre-legislative scrutiny is not a part of the legislative process but allows members of parliament to see proposals and consider general issues arising before the bill is finalised and formally presented to Parliament.

the proposal bears a marked resemblance to the proposal put forward by the Carnegie UK Trust (discussed in chapter 1.3. above). Significantly, the OHWP constituted a change from a focus on regulating the content of speech, or focusing on the host platform's immunity (or the conditions for loss of immunity). It was more orientated towards how the platforms operated and the impact of their features, as can been seen by issues that the OHWP raised for consideration: for example, down-ranking or reducing the visibility of content that has been disputed by reputable fact-checkers; improving the transparency of political advertising; promoting diverse news content; providing tools to users to help them protect themselves against harassment; steps to stop banned users from opening new accounts; tools to detect fake and spam accounts; processes to stop algorithms promoting self-harm or suicide content to users. The OHWP also envisaged improved process around take-down of content. The OHWP stated that there should be a regulator; Ofcom was confirmed as the regulator in the interim response. The powers of the regulator, as the experience of the ICO and the CMA have already demonstrated, are an important aspect of the regime especially given the asymmetry in information and resources between service providers and users.

The draft OSB imposes a number of duties on operators within scope, rather than a single over-arching duty of care, and in this there seems to be a difference even as regards the position in the FGR. The OSB imposes different obligations on "user-to-user services" and "search services". For both types of service, there is a difference between adult services and those likely to be accessible by children[81] which are subject to more stringent obligations.[82] It also seems that the OSB envisages reliance on age verification, though this is described in a technology neutral manner.[83] As regards adult services, all must take action in relation to "illegal content". Illegal content[84] comprises all crimes where the intended victim is an individual; the Law Commission was instructed to review the criminal law in relation to communications offences, with the expectation that the law may be revised to deal with issues such as abuse of intimate images. Terrorism and child sexual abuse and exploitation material are specifically mentioned (and have specific enforcement features[85]). Additionally, the Secretary of

81 That is, those under 18.
82 Content that is harmful to children is defined in cl 45 OSB.
83 Clause 26(3) OSB.
84 Defined cl 41 OSB,
85 Ofcom must produce separate codes in relation to terrorism and CSAEM and may use a "technology warning notice" Cl 63-68.

State may identify priority areas. Only 'Category 1' services – determined according to the FGR by reference to their level of risk[86] – need to take action in relation to content that is harmful to adults – that is, harm understood as a significant adverse physical or psychological impact on adults of ordinary sensibilities.[87] While not expressly mentioned in the duties, following the reasoning of the FGR[88] disinformation and misinformation that could cause significant harm to an individual will be within scope of content harmful to adults, a point reaffirmed by the fact that a committee is to be established to advise Ofcom on this issue.[89] It seems that some issues envisaged as within scope by the OHWP (eg transparency of political advertising) are not within scope of the OSB. Conversely, some concerns (online scams) that have been outside the proposed scope of the regime since the OHWP might not be included.[90]

Central to the regime is the idea that companies have effective systems and processes in place to understand the risk their services (including the design of those services) pose and to improve user safety; service providers are required to carry out and keep up-to-date risk assessments relevant to the types of content found on their service (an "illegal content risk assessment", a "children's risk assessment" and an "adults' risk assessment").[91] The service providers then have different duties to mitigate those risks. In relation to illegal content and to services likely to be accessed by children, a service operator must take proportionate steps to mitigate risks identified.[92] The requirements as regards 'harmful but legal' content ("adults' safety duty") seems limited to enforcing the Terms of Service, which need have no specific minimum content (save where "priority content"[93], "content of democratic importance"[94] and "journalistic content"[95] are concerned). Priority content must be specifically addressed, though the nature of this obligation depends of that category of content and, again,

86 The relevant provisions in OSB are cl 59 and Schedule 4.
87 Clause 46 OSB.
88 FGR (n. 79), para 2.82, 2.84.
89 CL 98 OSB
90 DCMS, Press Release: Landmark laws to keep children safe, stop racial hate and protect democracy online published, 12 May 2021, https://www.gov.uk/government/news/landmark-laws-to-keep-children-safe-stop-racial-hate-and-protect-democracy-online-published.
91 Cl 5(2), (4) and (5) OSB.
92 Cls 9(2) and 10(2) OSB respectively.
93 Cl 11(2) OSB.
94 Cl 13(4) OSB.
95 Cl 14(6) OSB.

the obligation in relation to the adults' safety duty is weak. Additionally, there are specific duties to have regard to freedom of expression and privacy. In addition, all companies in scope will have a specific legal duty to have effective and accessible reporting and redress mechanisms. They must also produce transparency reports (Ofcom providing guidance on form, content and process[96]).

Ofcom has a key role in understanding the nature of risk and the approach to mitigation and adding detail to the regime set out in outline in the draft OSB. It is obliged to carry out a risk assessment to identify, assess and understand the risks and develop risk profiles for different kinds of regulated services[97] and use that to provide guidance to service providers to assist them in their risk assessments. It is only after the guidance has been published that the regulated services will be required to carry out their risk assessments.[98] Ofcom will issue codes of practice in relation to the safety duties, as well as duties in regard content of democratic importance, journalistic content and reporting and redress. These codes will be subject to Parliamentary approval. Significantly, the Secretary of State has a power of direction to ensure that the code of practice reflects government policy or to ensure the protection of national security or public health.[99]

The OSB permits high fines (up to 10% global annual turnover[100]) and business disruption measures. These measures include the power to require providers to withdraw access to key services (and in this seem to be a development of the mechanisms in section 21 DEA) or, in the case of serious failures of the duty of care, to block the non-compliant service.[101] As in other areas of its remit, Ofcom will take a proportionate approach to enforcement. The OSB contains provisions in relation to criminal liability for company directors; these will only be brought into force if certain conditions regarding non-compliance with the regime are met. The regulator's decision may be challenged using judicial review principles.[102]

The regime also envisages a 'super-complaint' mechanism, whereby an 'eligible entity' may lodge a complaint with Ofcom about the existence of feature giving rise to significant harm to a large number of users.[103]

96 Cl 50 OSB.
97 Cl 61 OSB.
98 Cl 62 OSB.
99 Cl 33 OSB.
100 Cl 85-86 OSB.
101 Cl 91-94 OSB.
102 Cl 104 and 105 OSB.
103 CL 106-108 OSB.

There is no individual right of complaint in regard to a particular instance of harm to the regulator; a user in such a case should use the existing causes of action (against the person posting the content). In this there is a difference from the DPA18; whether follow-on actions (as seen in competition law as well as data protection) will be viable is unknown.

Chapter 10. Conclusions

This review demonstrates that the trend towards regulation of platforms exists, but that it is not one initiative but a multiplicity of actions in a range of policy spheres. This is not surprising given that there are elements of virtually all aspects of life online. Two questions arise: which are the lead areas; and how do the different sectors interact? This currently is uncertain given the present state of policy development, especially as regards the online safety agenda. The main regulators – the ICO, the CMA and Ofcom – are working together already which is essential to eliminate the risk of conflicting regulatory requirements and, as existing practice demonstrates, international cooperation will also be required. Despite potential overlap and tensions between regimes, a number of commonalities exist between them, notably the focus on the impact of design choices, and risk-based approaches to the applicability of the regimes.

A second similarity is the significance of the role of the regulators, and consequently the need for resources and appropriate powers. This is particularly noticeable with regard to the CMA and Ofcom, where new powers are envisaged to deal with digital markets; the ICO's powers have recently been extended, but that was driven by the GDPR. All regulators had general powers that were applicable to this field and which have been deployed to a greater or lesser extent. The existence of these powers is important given the need for legislation (at least as regards the CMA and Ofcom), and that progress particularly on online harms/online safety has been slow. In this, there is the difficulty of dealing with very rich companies and companies based outside the jurisdiction. Large fines are nothing new but there are indications that experimentation with enforcement tools, for example director's liability or director's disqualification as well as business disruption, is being considered but which may need legislative underpinning.

The final theme is the response, particularly of large companies, to enforcement of regulation. There has been a significant amount of litigation, draining the resources of the regulators and putting off the day on which the company must comply. This response, whether or not it is seen

as desirable, is hardly surprising – especially from 'long-pocket' litigants. The role and impact of collective litigation by users has yet to be fully understood.

Bibliography

Althoff, Juliane. "Crackdown in the online gambling sector." *Entertainment Law Review* 29, no. 1 (2018): 7-10.

Bevitt, Ann and Collins, Amy. "UK Enforcement: Top five focus areas." *Privacy & Data Protection* 20, no. 4 (2020): 10-12.

Brimsted, Kate. "All I want for Christmas is not to be sued (by you and you and you...)!" *Privacy & Data Protection* 21, no. 2 (2020): 6-10.

Caliskan, Samet. "Directors' disqualification in UK competition law: has the dog started barking?" *European Competition Law Review* 41, no. 10 (2020): 509-513.

Chijioke-Oforji, Chijioke. "Director accountability for breach of competition law: important practical lessons from the CMA's increased use of disqualification powers." *European Competition Law Review* 42, no. 1 (2021): 24-29.

Dunphy-Moriel, Marta and Dittel, Alexander. "A real-time bid to restore trust in online advertising: DMA's seven-step ad tech and other industry initiatives." *Entertainment Law Review* 31, no. 7 (2020): 233-236.

Geradin, Damien et al. "GDPR Myopia: how a well-intended regulation ended up favouring large online platforms - the case of ad tech." *European Competition Journal* 17, no. 1 (2021): 47-92.

Hon, Kuan. "GDPR's extra-territoriality means trouble for cloud computing." *Privacy Laws & Business International Report* no. 140 (April 2016): 25-28.

Jay, Rosemary. "The Age Appropriate Design Code." *Privacy & Data Protection* 21, no. 1 (2020): 3-7.

Jephcott, Mark and Karadakova, Vassilena. 'The CMA's increasingly expansionist approach to the share of supply test in UK merger control: a threshold issue." *European Competition Law Review* 41, no. 9 (2020): 466-475.

McDougall, Simon. Blog: "Adtech - the reform of real time bidding has started and will continue." January 17, 2020. https://ico.org.uk/about-the-ico/news-and-events/blog-adtech-the-reform-of-real-time-bidding-has-started/.

Sellars, Clare. "GDPR: one year on - ICO pulls back the curtain on the impact of the new regime." *Corporate and Trade Law Review* 25, no. 7 (2019): 172-174.

Shiner, Bethany. "Big data, small law: how gaps in regulation are affecting political campaigning methods and the need for fundamental reform." *Public Law 2019 (2):* 362-379.

Wenn, Christopher. "Can data protection solve the problem of microtargeting, manipulation of internet users and fake news?" *Entertainment Law Review* 29, no. 7 (2018): 216-218.