THE POST-PUBLIC SPHERE AND NEO-REGULATION OF DIGITAL PLATFORMS

CREATe Working Paper 2024/3

PHILIP SCHLESINGER

CREATe

The post-public sphere and neo-regulation of digital platforms[*]

Philip Schlesinger[**]

Abstract

This article discusses the post-public sphere and the regulation of platforms that have had disruptive effects on democracy. Platformisation means that the normative ideals for a political public sphere set out by Jürgen Habermas face a distinctive challenge. "Neo-regulation" is an evolving adaption by states that reflects the urgent need to address platformisation and digitalisation more generally. In conditions of geopolitical competition, notably between the China and US, attempts by various states and the EU to establish a neo-regulatory order has developed a significant national security dimension, which is highly relevant for the regulation of digital communication. Policing borders and content is an ever-present focus in all political regimes, whether characterised as democratic or authoritarian. Applying Pierre Bourdieu's field theory to internet regulation, the argument is illustrated by reference to current British regulatory practice. At the level of the state, the "regulatory field" is shaped by national and global forces. Although the British case has specific characteristics, the underlying analysis has general relevance for comparative research.

Keywords

geopolitics; national security; neo-regulation; platforms; post-public sphere; regulatory field

In loving memory of my brother, Ernest Schlesinger

[*] First published in *Javnost - The Public*, 2024 (Taylor and Francis). DOI: 10.1080/13183222.2024.2311010

[**] Philip Schlesinger is Professor in Cultural Theory at the Centre for Cultural Policy Research and Professorial Fellow at CREATe, the Centre for Regulation of the Creative Economy, both at the University of Glasgow. Email: Philip.Schlesinger@glasgow.ac.uk

> Public spheres are contingent on a whole range of presuppositions and, as such, they represent improbable evolutionary achievements of modern western societies. We cannot be sure that we will continue to enjoy them even in their countries of origin. Habermas (2009, 180-181)

Introduction

The digital space has increasingly become an object of regulation. The regulatory armature contends with a complex interplay of divergent forces within and outwith the territorial boundaries of the polity. The current drive to regulate media, communications and AI in the digital age is both global and national in reach: it occurs within democratic, authoritarian and hybrid forms of domination. My principal focus is on capitalist democracies and how regulation has increasingly taken centre-stage to address risks posed by digital communication. As will be discussed, this shift has provoked a major reappraisal in Jürgen Habermas's public sphere theory.

Colin Crouch (2004) has labelled the current state of capitalist democracies as one of "post-democracy," in which "all the institutions of liberal democracy [have] survived and functioned, but where the vital *energy of the political system … [has] disappeared into small private circles of economic and political elites" (Crouch 2019, 126). Liberal democracies, where the rule of law operates and intermediary institutions limit the exercise of executive power, are contrasted ideal-typically with populist democracies led by charismatic politicians who claim a direct relation to "the people" as they seek to evade the constraints of a democratic order. In line with this, Crouch (2019, 133-35) suggests that "xenophobic populism" – especially exploitation of déclassé citizens' fears of migrants and refugees – is likely to fuel post-democratic trends.

"Conspiracy theory is the logic of populism," David Runciman (2018, 65) has observed. Former President Donald Trump has been the contemporary arch-exponent of effective populist communications (Boczkowski and Papacharissi 2018). Trump's period in office added key terms to the political lexicon, with "fake news" and "alternative facts" signalling the entrenchment of a "post-truth" politics that has profoundly challenged rationalist nostrums about the value of evidence and civility in discourse (D'Ancona 2017; Wodak and Krzyzanowski 2017). Trump's term ended with his supporters' assault on the Capitol on January 6, 2020, and since then he has sustained an unproven claim that the US general election was stolen by a fraud on the American electorate. So far as public sphere theory is concerned, populist forms of communication (widespread internationally) constitute an epistemic challenge to normative assumptions about how to conduct democratic debate.

Given the focus of this article, the term "post-public sphere" is employed to designate an open-ended movement away from a "legacy'" media system in which, for decades, the press, radio and TV were considered the mainstays of mediated communications. The idea of a "hybrid" media system (Chadwick 2017) in which digital adaptations have occurred and reshaped legacy media is a useful staging post during a chronic and incomplete shift from one media and communications order to another. Widespread social media use has resituated, decentred, and reconstituted forms of formerly dominant political organisation and mass mediated public expression and consumption (Davis 2019). Platformisation has captured the bulk of the supply of traditional mass media content and, indeed, reshaped wider social relations (Van Dijck, Poell, and Waal 2018). How this transforming media ecology will evolve is an open question. As is illustrated by reference to the United Kingdom, one response to the complex expansion of the digital space is the development of neo-regulation.

Paolo Mancini (2023) has described such changes in party politics and media systems as "deinstitutionalisation," with legacy media largely replaced by social media, blogs, citizen journalism, tweets, and posts, transforming relationships between citizens and politics. Platformisation of the media ecology has taken a disaggregated, non-professional and non-institutional form. Consequently, the "reinstitutionalisation" that has occurred does not replace what went before. These processes are not internationally uniform (Reuters Institute 2023) but they do play out most profoundly at the level of the state.

In what follows, I first provide a sketch of the contested global context in which internet regulation is taking place. National security has become increasingly pertinent for states' regulatory policy. Digital regulation occupies a pivotal role in Habermas's analysis of the "new" structural transformation of the public sphere. However, although regulatory practice is invoked as an antidote to post-political trends it is neither described nor analysed. To address this absence, I have presented an illustrative analysis of recent British developments. Geopolitical and geoeconomic calculations have influenced regulatory policy's ramifying response to platformisation. Drawing on Bourdieu, this article develops the idea of a digital regulatory field. Discussion of national security brings both overt and covert regulation of the post-public sphere into focus.

Communicative Space in Contest

The global history of post-war media development was initially shaped by Cold War geopolitical struggles for influence. Models of the press disseminated during the Cold War still influence discourse in the digital age. Opposed models of "libertarian" and "Soviet" media organisation and control (Siebert, Peterson, and Schramm 1956) played into propaganda warfare between the

blocs led by the Soviet Union and the United States and have contemporary echoes (Rantanen 2017).

A decade before the collapse of the Soviet Union, UNESCO adopted the MacBride Report (1980), advocating a New World Information and Communication Order (NWICO), which challenged US and other western powers' media and cultural dominance in global marketplaces (Golding and Harris 1997; Schlesinger 1991, chap.7). The US and UK withdrew their support from UNESCO "to undermine the legitimacy of multilateral principles of global media governance and cultural policy that were not guided by market principles that serve big media interests" (Calabrese and Mansell 2023, 214). Advocacy of the "free flow of information" during the Cold War reflected the deep strategic connections between communication and national security (Mattelart and Mattelart 1992 [1986], 160-163).

With the shift to a global neoliberal regulatory regime UNESCO's stance changed (Calabrese and Mansell 2023, 215; Chakravartty and Sarikakis 2006, 36–37). Dividing lines of global debate were redrawn with the advent of the internet. Backed by United Nations bodies, for two decades the World Summit on the Information Society (WSIS) – a self-described "global multistakeholder platform" for sustainable development – has linked a chain of initiatives. WSIS's framing pitch was geoeconomics rather than geopolitics, with a key distinction drawn between "the developed and developing societies" (WSIS 2005, 11). In its call for national and international "digital solidarity," the internet was depicted as "a central element of the infrastructure of the Information Society … a global facility available to the public" (WSIS 2005, 75). Beyond its possible public uses, however, infrastructure's role in national security is presently much in evidence.

Continuities exist between the platform era and Cold War divisions. Supersession of the Open Internet and the weakening of internet governance modelled on a liberal democratic market-dominated order have clarified current geopolitical fault lines (Flew 2021, chap. 6). Van Dijck, Poell, and Waal (2018, 26) have summarised the key present-day divide: "The American and Chinese ecosystems dominate their own geopolitical spheres and are rooted in opposing ideological views."

Distinct legal and administrative traditions shape diverse approaches to how the internet is governed. O'Hara and Hall (2021, chap. 7) stress EU official values, in particular preserving human rights and dignity and taking a precautionary approach to possible harms. Advocates of a "European" approach based in public values stress the priority of citizens' needs over those of global corporations, and effective regulation of US big tech corporations is high on the agenda

(Van Dijck, Poell, and Waal 2018, 165-66). They compare this to the US's libertarian approach, which prioritises freedom of speech and association over privacy. The commercial internet, which has such a globally dominant role – led by big tech corporations such as Alphabet/Google, Apple, Amazon, Meta/Facebook and Microsoft – is made in America (O'Hara and Hall 2021, chap. 9). In 2023, a notable antitrust action was initiated against Amazon's pricing by the Federal Trade Commission, signalling new regulatory activism (Faroohar 2023).

The EU has achieved international prominence as a regulatory space and is notably active in areas such as privacy, copyright, and data protection. The General Data Protection Regulation 2016 (GDPR) has transcended international boundaries, projecting EU soft power. Risks to democracy deriving from cross-border interference in national elections, "misinformation" and "disinformation" campaigns during the Covid-19 pandemic, and populist uses of digital media have posed new regulatory challenges (Trappel et al. 2024). One response was to set up the High-Level Expert Group on Fake News and Online Disinformation in 2018. Key EU regulatory initiatives have included the Digital Markets Act 2022, focused on "gatekeepers" most prone to unfair business practices, and the Digital Services Act 2022, which aims to regulate "very large online platforms." The European Union's AI Act, still to come into force, is a global first, providing a legal basis for a risk-based approach to regulation. By comparison, the US's regulatory instruments for AI are still widely distributed across federal agencies (Engler 2023).

In China, the internet is subject to goals set by the Chinese Communist Party, and focused on achieving national autonomy in tech, cyberspace, and the online environment. Expanding regulation of online harms is on the agenda. The system is characterised by overt censorship and monitoring. The major tech players, Huawei, ZTE, Lenovo and Xiaomi, and key platforms, Alibaba, Baidu and Sina Weibo, are ultimately subject to state oversight. However, top-down control is coupled with considerable technological innovation that rivals that of the US (O'Hara and Hall 2021; Flew 2021). China, which has developed considerable capacity in AI regulation seeks global leadership in that field (Sheehan 2023).

Taking stock, Terry Flew (2024: 166; original emphasis) notes that "In the 2020s … we find ourselves in an era that is less about whether to regulate the Internet, but how a *regulated Internet* should operate, and who should take responsibility." Struggles over the modes and scope of regulation will not disappear as the drive to regulate develops further within democratic, authoritarian and hybrid forms of domination. Today's *intensified* regulation is symptomatic of the crisis management of communicative space by national states in a contested global order.

For instance, there is growing competition to shape international policy development for AI: in late 2023, the UK organised a summit of 28 governments to influence global network governance. This coincided with the US's creation of an AI Safety Institute (Department of Commerce 2023). The ensuing Bletchley Declaration highlighted "safety risks of shared concern" and the pursuit of "risk-based policies across countries" (Department for Science, Innovation & Technology 2023). Both China and the US were represented, as were Australia, India, and the EU. It remains to be seen how governance evolves in this rapidly developing field.

Public Sphere Theory and Internet Regulation

Habermas's (2023 [2018-22]) contemporary analysis of a "new structural transformation" addresses the far-reaching impact of the internet on the political public sphere. His classic account of the public sphere was conceived in a different era. The demise of the bourgeois model, he argued at the time, was due to "the structural transformation of the relationship between the public sphere and the private realm" (Habermas 1989, 142-43). Interventionism by social-welfare states meant that "state and societal institutions fused into a single functional complex that could no longer be differentiated according to criteria of public and private." In post-World War II democracies, the political public sphere had become "manufactured," "manipulated," "mass-media dominated," limiting the normative ideal of rational deliberation by a public (Habermas 1989, 148; 216-17).

Unregulated Exchange. In Habermas's subsequent reflections on political communication in a "media society," he suggested that "given the revolution in electronic communication, the deliberative paradigm is well suited to relating the strong normative ideas to present-day social complexity" (Habermas 2009 [2008], 143). Deliberation is described as "a discursive filter-bed which sifts interest-generalizing and informative contributions to relevant topics out of the unregulated processes of opinion-formation." Filtered proposals emerge as responsible "public opinion." Political public spheres have a distinctive role within wider national public spheres that are far more diverse in cultural expression and modes of consumption. The political public sphere exercises "a centripetal force" by synthesising a tested selection of publicly relevant ideas. It provides an agenda for citizens at any given time. Habermas (2009, 155-56) stresses the disciplined application of evidential standards to filter and test public opinion.

Crucially, Habermas argued that internet-mediated communication resulted in "unregulated exchange" between partners in an unregulated, commercially run system that produced fragmented national publics. By comparison, "media-based mass communication" (via press, radio, and television) remained the keystone of the political public sphere. However, dominated by political elites and experts, such asymmetrical public communications required legitimacy.

Genuine journalistic independence required self-regulation, whereas for their part citizens needed to participate actively in political discourse (Habermas 2009, 173). It was acknowledged, however, that media systems are prone to party political interference, power-enhancing concentrations of ownership, covert influences, the commercialisation of public service broadcasting, and the rise of prototypical media populists such as (at that time) the Italian media magnate and prime minister, Silvio Berlusconi – a key media-political forerunner of Donald Trump's. In short, as ever, a gap existed between normative ideals and empirical realities.

A decade and a half later, Habermas (2023) underlined the far-reaching implications of digitalisation for a political public sphere in democratic systems faced by a profound crisis of credibility. He stressed the fundamental contribution of "political communication in the public sphere … to the democratic process," reaffirming the importance of deliberation while lamenting the "decline, and in some countries almost the demise, of [the] rationalising power of public debates." Digitalisation of public communication was undermining the inclusive and intensive character of the public sphere, threatening even minimal "civic solidarity" (Habermas 2023, 23; 32).

For Habermas (2023, 36-39), then, the shift of mass news consumption to social media often functioning as echo chambers had opened to the door to populists' exploitation of disaffected voters. The national public sphere was underserved by "unregulated communication processes" and "unregulated content" lacking professional journalistic filtering. Platformisation produces "fragmented" and "unbounded" public opinion. "Generalised authorship" lacking intermediation by journalists is distributed by global corporations without a stake in the national public sphere, with traditional media losing influence.

The Epistemic Threat. Habermas (2023, 51; original emphasis) argues that "the customary conceptual *distinction between public and private spheres*" and the "self-understanding of internet consumers as citizens" is in jeopardy. In short, some citizens' risk self-exclusion from engagement with the national public sphere, to the detriment of all. The chances of a common agenda of "topics that deserve *shared* interest" are diminishing in a public media culture "whose reliability, quality and general relevance" is in question (Habermas 2023, 52-53; original emphasis).

Rather than accept this as a structural transformation of the public sphere, Habermas stresses that:

> the societal basis for a separation of the public sphere from the private spheres of life has not undergone any essential changes. Nonetheless, the more or less exclusive use of social media may have led in parts of the population to a change in the *perception of the*

> *public sphere* that has blurred the distinction between 'public' and 'private', and thus the inclusive meaning of the public sphere. (2023, 53; original emphasis)

The crisis is interpreted, therefore, *not* as a structural question but as effective self-exclusion from the public sphere by those whose modes of consumption distance them from the value of rationalising discourse. At the same time, platforms have achieved "*the epistemic status of competing public spheres*" (Habermas 2023, 45; original emphasis) with users of the internet "empowered as authors" who challenge the value of professional journalism. This situation is variously designated a "plebiscitary public sphere," an "unstructured public sphere," and a "semi-public sphere" (Habermas 2023, 57). These multiple descriptors do not clarify the situation. Without naming it, Habermas has described the preconditions of a *post*-public sphere (Schlesinger 2020).

Habermas (2023, 59) calls for a "constitutional imperative" to re-establish "a media structure that enables the inclusiveness of the public sphere and the deliberative character of public opinion and will formation." This formulation signals a state of emergency. In a reversal, former border-transcending aspirations for a European public sphere and cosmopolitan post-national citizenship have ceded place to the nation and the state (Fossum and Schlesinger 2007; Habermas 1996, appendix 2; 2009, 181-83). Democratic *national public spheres* are now identified as key sites of struggle because "the centralized state organizations with the power to act" are "for the time being limited to national territories" (Habermas 2023, 35).

Regulation as an Antidote. Habermas (1996 [1992], 442; original emphasis) has long advocated the principle of "constitutional regulation of the *power of the media*" for a well-functioning political public sphere. This position expressly countered the deregulation pursued by neoliberal policymaking, which engendered the privatisation of state-owned industries, "flexible working," and "withdrawal of the state from many areas of social provision" (Boltanski and Chiapello 2005 [1999]); Harvey 2005, 3). Pertinently, privatisation and deregulation reshaped telecommunications and broadcasting (Mattelart and Mattelart 1992 [1986], chap.14), whereas market competition enabled concentrations of ownership and corporate power (Keane 1991). As neoliberal doctrines adapted to the "uneven geography of political economic influence" (Springer 2016, 22), national contexts have retained their specificity.

Three decades ago, public sphere theory was used in the left's defence of public service broadcasting's role in sustaining "the public interest and civic culture" (Livingstone and Lunt 2013, 90). Garnham (1994, 362) then noted the "progressive destruction of public service as the preferred mode for allocating cultural resources." Currently, in several countries public service media (steadily morphing into public service streaming) have faced a loss of trust and cuts in

funding. Moreover, the "quality" newspaper, totemic for Habermas, is largely eschewed by digital natives (Reuters Institute 2023).

Regulation of the internet by states has become important for public sphere theory late in the day, given that this has been on the agenda for well over two decades in the field of political communication (Street 2001, 122). Habermas's new emphasis on regulation is gestural and leaves others to fill in the gaps. His latest work contains the sole critical observation that EU competition regulation is inappropriate for correcting platforms' deceptive communications (Habermas 2023, 58).

The National Security Paradigm. Regulatory activity is shaped by the type of regime in which it is situated and institutionally marked by the prevalent legal and political culture. As current developments reflect each state's geopolitical situation, policy making is underpinned by a "national security paradigm" that "emphasizes the military power and autonomy of the state, which is always defined in relation to the power of other states." Crucially, the "national securitisation" of regulatory policy depends on "recognition of cyberspace as a military domain and the reframing of cybersecurity as a problem of *national* security" (Mueller (2017, 74; original emphasis). Advocacy is required for a policy of national securitisation to be adopted (Bevir and Hall 2011). Not surprisingly, "digital sovereignty" is moving up the agenda of research on nationalism and communications (Mihelj 2023).

This focus is not new, however, as almost half a century ago Armand Mattelart (1979 [1976]) documented Cold War struggles over control of the militarily sensitive international trade in electronics. Chris Miller (2022) has labelled the contemporary contest a "chip war." As we shall see, global competition between China and the US has shaped the UK's approach to imported semiconductor technology. Aside from their role in industrial policy and competitive trade, the protection of infrastructure is also a precondition for the operation of a national public sphere.

Since the 1940s, the US has adopted a national security approach. Employment of this framework by a hegemonic power has shaped international trade with allies and adversaries during the Cold War as well as current geopolitical rivalry with China. Daniels and Krige (2022, 7) put it succinctly:

> Export controls are just one of an increasing, and increasingly invasive, regulatory system devised by the architects of the US national security state to restrict the flow of information, people, and commodities across the national border to friend and to foe alike.

During the Cold War, national security was a driving force in the creation of the internet, initially conceived as a secure communications system (Nieminen, Padovani, and Sousa 2023). Consequently, concern about hi-tech led to the incorporation of economic security into US national security doctrine (Daniels and Krige 2022).

The State as an Analytical Focus

Amidst an international repertoire of policy measures, national political and legal cultures matter greatly. The state remains a classic starting point for comparative analysis and a locus for assessing how global forces shape national developments. For instance, in a related field, I have shown how transnational framings of domestic British film policy came about through UK industrial ties with Hollywood and EU media programmes. Such international connections shaped the recruitment of key actors and decisions made in the major British film agency (Schlesinger 2015).

A caveat is required when taking the state as a starting point for investigation. This does not mean embracing "methodological nationalism" (Beck 2006). Rather, although regulatory institutions might be designated "national" they are substantially shaped by forces external to the boundaries of the state. Fiona Adamson (2016, 23; 25) advocates a "spatial turn" that requires us to recognise that "territorial nation-states [are] only one of many 'spaces' that are constituted through practices of violence". Cyberspace, moreover, "is an arena in and of itself in which forms of politics take place": platforms occupy precisely the global space that states are seeking to regulate. In practice, national regulatory strategies interact with "global webs of regulatory controls" (Braithwaite and Drahos 2000, 550). Thus, global regulatory and security concerns may be incorporated into national ones at the level of the state. The discussion of UK regulatory developments that follows assumes that, in a reverse movement, analysis of national particularities may play into the development of general theory (Wacquant, 1996: ix).

My colleagues and I tracked the British debate over platform regulation as it had developed in parliamentary hearings and government-commissioned reports, while engaging regulators in dialogue (Kretschmer, Furgał, and Schlesinger 2022). By 2020, a "neo-regulatory" approach had crystallised. "Neo-regulation" is a term intended to capture how policymaking seeks to address the expanding range and scope of platforms' activity (Schlesinger 2022). In the UK, the response foregrounded two portfolios with some crossovers: "online safety" on the one hand, and competition and innovation on the other. Since that research began, AI regulation has increasingly come into focus, although in Britain – unlike the EU – at present, it still awaits legislation.

UK neo-regulation has also been influenced by Brexit, the state's "Global British" nationalist turn after quitting the European Union, first summed up in the government's *Integrated Review of Security, Defence, Development and Foreign Policy*, published in March 2021 and "refreshed" in March 2023 (HM Government 2021; 2023). This "vision" encompassed views on the state, polity, economy, and social order in a totalising social imaginary that reprised the axial Cold War distinction between democracies and dictatorships, naming Russia and China as key adversaries.

The UK Government's *Integrated Review* describes a state in which digital infrastructure is a linchpin of the economy, the state's global competitiveness, and national security (Department for Digital, Culture, Media & Sport 2022). The state is portrayed as engaged in competition for global digital market dominance and diplomatic influence. In an exercise of soft power, regulatory diplomacy should be used to "influence the rules, norms and standards governing technology and the digital economy" (HM Government, 2021, 20). As elsewhere, the geopolitical role of major non-British tech companies operating inside the national territory is subject to security service vigilance: critical national infrastructure is a key asset to be defended.

Some contend that public service media (and sometimes the media more generally) should be conceived as an "infrastructural" resource that is "a necessary precondition for public opinion to emerge," a support for spaces of representation and expression conducive to a functioning public sphere (Gripsrud and Moe 2010; Splichal 2022, 28). At a time of global poly-crisis, this perspective will find it hard to avoid being incorporated into the state's wider mission of infrastructural defence.

Platforms and infrastructure are deeply interconnected. Van Dijck, Poell, and Waal (2018, 12-13) have described infrastructural platforms – those owned and operated by Alphabet/Google, Apple, Amazon, Meta/Facebook and Microsoft – as forming "the heart of the eco-system upon which many other platforms and apps can be built. They also serve as online gatekeepers through which data flows are managed, processed, stored, and channeled." Plantin and Punathambekar (2019, 164) observe that "an infrastructural optic reframes the study of digital platforms" which are key sites for the analysis of regulatory policy and state power.

The value placed on infrastructure by national security doctrine extends to how national communicative space is being reconceived. Larkin (2013) reminds us that calling something "infrastructural" requires selective denomination. Consequently, how infrastructures are given meaning through frameworks of interpretation – their poetics – plays into the politics of national identity, how states symbolise their defensive capacities, and their modes of patrolling the

boundaries of culture and identity. This relates infrastructure to debates about the protection and enhancement of media production under conditions of cultural and economic dependency in a global marketplace.

The Neo-Regulatory Apparatus

Flew (2021, 164) has described the regulation of platforms as concerning "the laws, policies, and agencies of nation states, including supranational regulatory entities such as the European Union." Much of the account that follows concerns the role of "regulatory rule-makers" based in "public agencies with a clear legislative mandate and formal mechanisms of monitoring and enforcement" (Levi-Faur, Kariv-Teitel, and Medzini 2021, 2). However, alongside the work of agencies, it is argued here that we need to rethink more precisely how executive and legislative actions taken by government fit into the picture. In short, we need to enlarge the scope of our account of regulatory action, as is demonstrated below.

Key players. In the UK, in the foreground of attention, government-commissioned inquiries and task force reports fed into the recalibration of regulatory capacity. A hierarchy of regulatory bodies emerged from our analysis of the 2018-2020 "issue-attention" cycle (Downs 1972). However, in the extensive paper trail analysed, we noted that national security had received relatively little attention (Kretschmer, Furgał, and Schlesinger 2022).

In 2020, the agencies given a crucial role in regulating internet platforms were the Office of Communications (Ofcom), with a wide role in media and communications regulation; the Competition and Markets Authority (CMA), the key competition regulator; and the Information Commissioner's Office (ICO), focused on data protection. All have statutory status; they report to the UK Parliament; and exercise enforcement powers. In 2020, at their own initiative they set up a new collaborative entity called the Digital Regulators Cooperation Forum (DRCF). A further statutory body, the Financial Conduct Authority (FCA), which regulates the UK financial services industry, joined the existing troika in 2021.

The purpose of the regulators' forum is to achieve a consortial approach to regulation by sharing information. It also aims to inform regulatory policy making, look ahead, promote innovation, and strengthen international engagement. The creation of the DRCF was a pre-emptive response by regulators to head off political pressure, notably from the UK Parliament's upper chamber. The House of Lords Communications Committee had proposed establishing a statutory Digital Authority to oversee the regulatory landscape. The DRCF is a noteworthy instance of administrative invention by statutory bodies. It fits an established British model known as "concurrent regulation," where agencies with related remits work together (Schlesinger 2022).

So far, despite initial doubts about its international attractiveness (Dunne, 2021), the British model has been adopted in Australia and the Netherlands (Vanberg 2023). The DRCF has its own secretariat and CEO. Its joint programme of work for 2022-23 included child protection online; promoting competition and privacy in advertising; supporting improvements in algorithmic transparency; and enabling innovation in the regulated industries. AI is firmly on the agenda for 2024.

Julie Cohen (2016, 21) argues that movement from industrial to informational capitalism has resulted in major shifts in regulatory practice and its legitimations. Her analysis demonstrates a shift from "traditional administrative law" in the US to various forms of "creative institutional entrepreneurship," including in platform regulation. The DRCF is an instance of such adaptation, although it remains to be seen how effective the UK's neo-regulatory arrangement will be in addressing major platforms' economic, political, and communicative power.

The Online Safety Bill was introduced to the UK parliament on 17 March 2022 after a long delay, due to political turbulence in successive Conservative governments, coupled with push-back from a range of interests. It became law on 26 October 2023. The Online Safety Act (UK General Public Acts 2023) imposes a statutory duty of care on platforms. It seeks to manage the risks of harms to users that derive from illegal content and activity, with special emphasis on the protection of children. Ofcom has been tasked with regulation and has set up a 350-strong team for this purpose (Criddle 2024). Some 100,000 services are like to fall into regulatory scope and the Act will not be fully operational until 2025 (National Audit Office 2023).

Although online safety has dominated the headlines, competition is also firmly on the UK policy agenda. In 2019, Jason Furman, a Harvard economist, headed a government review of digital regulation. A "pro-competition regime" was proposed for the most significant digital platforms with so-called "strategic market status" (SMS). The main targets were Facebook and Google, which have jointly dominated UK advertising, search, and social media use (Digital Competition Expert Panel 2019). The pivotal competition regulator, the Competition and Markets Authority (CMA), steered the digital markets strategy.

The Furman review recommended establishment of a further regulatory body: the Digital Markets Unit (DMU), tasked to focus on dominant platforms. The DMU was set up as a pre-statutory body within the CMA. After much delay, on 25 April 2023 the Digital Markets, Competition and Consumers (DMCC) Bill was introduced to the UK Parliament. The provisional plan is for the DMU's effective regulation of SMS using "pro-competition interventions" to begin in July 2025, with some 200 staff presently assigned to this purpose. Once implemented, the

regulator's planned *ex ante* approach will be comparable to EU regulation of "gatekeepers" and "very large online platforms," as well as to approaches planned in Australia and Germany (CMA 2024).

The Regulatory Field

The UK's approach to internet regulation has been dominated by pragmatic coordination between multiple agencies' strategies. Michael Moran's (2004) view that the British state is prone to "hyper-regulation" is borne out by the plethora of actors involved. Agencies depend either on their creation by the state or recognition that officially endorses a body's (and its agents') claims to relevant competence. Those at the apex of regulation enjoy the highest level of public "consecration," to use Pierre Bourdieu's (1996 [1989], 118) term: such bodies have "a legally recognized capacity to wield a form of power that is effective because it is legitimate". The most consecrated bodies have statutory powers, with public bodies such as the regulators described above exercising their powers on an "arm's-length principle" usually described as "independence". In British political culture, this symbolically important claim signifies autonomy from direct political influence.

British regulatory agencies may be conceived as occupying a distinct relational space – a field – shaped by the exercise of state power and its interaction with global platform power (Helberger 2020). Bourdieu (1993 [1968-97], 162-64) influentially described a field as "a separate social universe having its own laws of functioning independent of those of politics and the economy." It may be seen as "an autonomous universe endowed with specific principles of evaluation of practices and works" and "specific laws of functioning within the field of power." As suggested in our earlier work, this conceptualisation is highly pertinent for analysing regulation (Schlesinger 2020; Kretschmer, Furgał, and Schlesinger 2022).

Bourdieu's (1986 [1979]) use of field theory is best known for analysing relations between cultural practices and social tastes. Its pertinence to the present analysis does need some argument. The "regulatory field" differs from those in which cultural actors and consumers strive for distinction in expressing differentiated tastes. Instead, it concerns agencies whose decisions claim legitimacy by reference to their expert applications of legally enforceable codes and rules. Moreover, regulators' specific "rules of functioning" in respect of the economy and politics vary significantly according to how they are positioned within the field. Furthermore, only some of those engaged in regulation conceive of their actions as "independent," in line with their constitutive statutes, and even then, they do recognise their autonomy operates within defined limits. In one part of the field, therefore, statutory regulators endowed with specific remits are indeed relatively autonomous from executive power, while non-statutory agencies are diversely

authorised by the state to perform their tasks. Finally, in countering state and non-state adversaries in the name of national security, regulation is highly proximate to centres of executive power, whereas threats to critical infrastructure or state secrecy may involve either direct intervention in the economy or using cyberwarfare.

With these provisos in mind, we may analyse the division of labour distributed across the clusters of agents and agencies occupying a regulatory field in which power subordinate to that of the state is exercised. As Bourdieu puts it, regulators possess a "dominated" form of diversely distributed power. As in cultural fields, those involved in the regulatory field are engaged in the critical evaluation of *practices* (such as anti-competitive action, or failure by self-regulated enterprises to meet their terms and conditions of service) and of *works* (such as the multifarious content distributed by platforms). Each agency may undertake innovation but only within the scope permitted (Emirbayer and Johnson 2018, 14-16).

As in other jurisdictions, the UK system's patchwork-quilt is marked by competition for regulatory influence. The three agencies that co-invented the Digital Regulators Cooperation Forum (DRCF) jointly defined the neo-regulatory challenge as requiring concurrent operations. At the same time, this move established a collective institutional interest in defining and protecting a collaborative space from unsolicited entry by others seeking to compete in defining the agenda (Digital Regulators Cooperation Forum 2021). To date, the DRCF's strategy has successfully held at bay both politicians demanding greater parliamentary accountability and sources of competing expertise avid for a seat at the regulatory table (Vanberg 2023). This may change. There is plainly a public interest both in setting up and efficiently articulating wide-ranging regulatory capacity and capabilities to address rapid changes in digital technologies. For instance, although a UK regulator has not yet been established for AI, an AI Safety Institute was launched at the Bletchley Summit in November 2023, creating a further source of advisory expertise, adding to that already widely distributed across government departments and specialist agencies. This has resulted in "a complex, multi-layered set of guidelines and regulation from multiple bodies" (Shepley and Gill 2023, 1). The DRCF is presently positioned to play a significant multi-regulator coordinating role through an AI and digital hub.

The British field of platform regulatory power ranges over competition in the digital economy to politics and social life close to the classic concerns of public sphere theory. In principle, statutory bodies are held accountable by the executive and parliamentary committees. However, this is just the most *visible* area of the regulatory field. I therefore propose that we enlarge our conception of its constituent parts. Neo-regulation also includes *covert* or largely

discreet relations between national security bodies, regulators, key media, and major platform players.

Moreover, regulators' relations with the political world do not exhaust the totality of the regulatory field. A comprehensive analysis needs to examine how it structures relations *between* regulators and a range of "stakeholders" such as regulated platforms; industrial and occupational lobbies; expert circles of professional analysts, academics, and think-tanks; and at times, issue-focused interest groups or individuals (Neudert 2023). Knowledgeable intervention counts greatly in shaping policy, but it has high costs of entry.

A stake in the game is to exercise "convening power." The UK government, like its counterparts, sees leverage over platform regulation as an asset for its soft power ambitions; the Bletchley AI Summit was a case in point. Despite the political distance taken from the EU since the Brexit vote, British regulators have remained closely connected to their European Union counterparts. International connections, especially with "like-minded countries," as the current phrase has it, are important in developing regulatory policy and transnational governance.

Regulation in the Shadows

An exclusive focus on regulation undertaken by the DRCF's agencies obscures the real work of the regulatory field. Both national security legislation and special-purpose regulatory arrangements need to be included. This reflects the concerns of public sphere theory. Habermas (1996, 433) has contended that the general duty to protect citizens in welfare states has resulted in "building up and arming the constitutional state to the point where it becomes the 'security state.'" Surveillance, he argues, developed in line with politicians' and officials' expanding perceptions of dangers to the social order. This security-oriented mind-set may engender convergent interests between government and big tech, as Runciman (2018, 154) notes: "Democratic states like the US and Britain have turned out to be prolific accumulators and hoarders of metadata." Relatedly, Shoshana Zuboff (2019, 113-15) argues that Al-Qaeda's 9/11 attack on the US influenced the Federal Trade Commission's intention to regulate internet platforms' infractions of online privacy. Subsequent adoption of a "harms-based" approach that allowed platforms to self-regulate coincided with enhanced collaboration between national security agencies and big tech in data mining for national security and intelligence purposes. This raises questions about how effectively the watchers are being watched and required to account for their actions.

Trade Policy as Regulation. A focus on national security contributes to an expanded conception of the regulatory field, as illustrated by the UK's response to US trade policy. Daniels and Krige

(2022, chap.10) discuss how, in 2019, Chinese-owned Huawei, the largest global telecommunications equipment provider and second-largest producer of smartphones, became "blacklisted" by the Trump administration's use of the US export control system. This had far-reaching commercial consequences for other companies, including Google's operating systems, mobile parts manufacturer Lumentum Holdings, and key international computer chip producers. As Daniels and Krige (2022, 300; original emphasis) remark, "The Huawei case became, during the Trump years, *the* public symbol of the US-China clash, and it rapidly changed the political economy of global knowledge sharing." Fundamentally, the US Government saw Huawei as an agent of the Chinese state and a risk to US critical infrastructure. Consequently, the company's intended investments in American companies were blocked.

The repercussions were rapidly felt across the Atlantic. In January 2020, the UK's National Cyber Security Centre (NCSC) identified Huawei as a high-risk vendor for the UK's planned 5G cellular network upgrade. Using the National Security and Investment Act 2021 (NSIA) to exclude communications technology deemed to carry risks to critical national infrastructure, the UK government decided to fully remove Huawei as a supplier by 2027. In 2010, the Huawei Cyber Security Evaluation Centre had been set up to manage the state's relations with the tech producer (HCSEC 2020). In this arrangement, NCSC, acting for the government, liaises closely with the national security and intelligence agency, Government Communications Headquarters (GCHQ) (Cabinet Office and National Cyber Security Centre 2021). This set-up is a form of infrastructure regulation, although it is not widely discussed in those terms. Legislation, therefore, was combined with setting up a special-purpose agency to regulate sensitive trade.

In November 2022, the UK government also blocked the purchase of a British semiconductor producer based in Wales, Newport Wafer Fab. If taken over, the company would have come under full control of Nexperia, a subsidiary of the partly Chinese state-owned company, Wingtech (Thomas 2022). Once again, national security grounds were invoked under NSIA 2021. Such intervention in the market may also legitimise anti-competitive protectionist decisions. Under NSIA 2021, fourteen Final "Orders to Exclude" were issued in 2022 (HM Government 2023, 48-49) in line with British Prime Minister, Rishi Sunak's concern about "high-risk investment in critical infrastructure and sensitive technologies" (HM Government 2023, 3).

The exercise of ministerial powers to regulate in this way is not hamstrung by a stakeholder model, public consultation, or regulators' in-house deliberation. An executive approach therefore differs from "arm's-length" regulation by a statutory body. The use of legislation by ministers to ban technology is a further feature of the regulatory field.

The Take-down as Regulation. Our analysis of the policy paper trail drew attention to an anomalous body. The Counter-Terrorism Internet Referral Unit (CTIRU) is formally part of London's Metropolitan Police Service. Its role is to remove illegal online content both globally and in the UK that breaches UK terrorism and counter-terrorism legislation. It engages with industry and private sector companies by focusing on breaches in websites' terms of service. Given its national security status, little public information exists on a private body originally set up in 2010 by the Association of Chief Police Officers (Kretschmer, Furgał, and Schlesinger 2022, 22-23). As Sissela Bok (1982, 115) remarks, national security is a "code word" used "to create a sense of self-evident legitimacy," supporting "collective practices of secrecy."

CTIRU evidently reports to the Home Office (the UK's Ministry of the Interior): since its formation, the department's ministers have answered to Parliament on its behalf. Parliamentary questions may elicit overall figures on the removal of "extremist and terrorist" content. For instance, on 19 July 2019, a minister reported that CTIRU had "secured the removal of over 310,000 pieces of terrorist material since its inception in February 2010" (Atkins 2019). On national security grounds, ministers have refused to disclose the size of CTIRU's workforce or the funding allocated for its work; no comprehensive data exists on services affected by take-down referrals (Hayes 2014; Open Rights Group 2023).

CTIRU's role is anomalous only when judged by the criteria applied to high-profile, fully accountable regulation. Its existence prompted me to rethink the scope of the regulatory field, consequently including low-profile activity with a primarily national security dimension. By contrast, UK legislation on terrorism also underpins the regulatory practice of Ofcom under the Online Safety Act 2023, but for that body national security is just one key enforcement task among many.

The UK's Internet Referral Unit (IRU) has been adopted internationally as a model of "informal governance." Eghbariah and Metwally (2022, 587) have noted that "IRUs manage a new system of governance in which laws are replaced, or rather supplemented, by terms of service and the judiciary by companies' content reviewers." The EU's IRU is based in Europol; France has an *Office centrale de lutte contre la criminalité liée aux technologies de l'information et de la communication* (OCLCTIC); and Israel operates a Cyber Unit in the Office of the State Attorney. Reportedly, similar units operate in Austria, Belgium, Italy, the Netherlands, Spain, and Switzerland (Eghbariah and Metwally 2022).

Government Information Management as Regulation. The UK Government Communications Service (GCS) aims to deliver "an effective national security communication capability as envisaged in the Integrated Review" (Government Information Service 2020, 3). The public health emergency engendered by the Covid-19 pandemic was also a democratic crisis in which the deployment of "disinformation" and "misinformation," identified as coming from Russia, a prominent source of cyberwarfare (O'Hara and Hall 2021, chap. 13), challenged the government's primacy in information management.

The GCS focused on supporting the lock-down and protecting the health service. It used its Rapid Response Unit (RRU) – set up in the Cabinet Office in 2018 – to rebut "false narratives" regarding coronavirus (Cabinet Office and Department for Science, Innovation and Technology 2023). Ministers described the RRU as a small unit that "monitored news and information being shared and engaged with online, using only public and openly available information to do so." Its analyses were distributed within government (Burghart 2023; Cabinet Office and Department for Digital, Media & Sport 2020).

During the pandemic, a Counter Disinformation Unit (CDU) – previously used in 2019 to monitor online material during the UK and EU election campaigns – was revived. It was based in the Department for Digital, Culture, Media and Sport (DCMS). The CDU, established on 5 March 2020, was set up to counteract the dissemination of false information regarding Covid-19. It reflected Cabinet Office concern about "certain states," clearly including Russia, although that was not stated (Cabinet Office and Department of Digital, Culture, Media and Sport 2020). Like CTIRU, the CDU focused on content deemed to have breached platforms' terms of service. This period saw "heightened state-platform interplay, as the government and platforms collaborated to combat information threats." Cooperation included a joint public health information campaign and convening a range of stakeholders, including platforms, in a Counter Disinformation Policy Forum (Neudert 2023, 11).

A DCMS minister informed the House of Lords Democracy and Digital Technology Committee that the CDU's personnel came from the Home Office, Foreign and Commonwealth Office, and Cabinet Office, and included Ministry of Defence "military analysts". On national security grounds, "tactics or approaches" were not made public (Dinenage 2020). According to the Chief of the General Staff, General Sir Nick Carter, the British Army's 77 Brigade – specialists in psychological warfare and Russian misinformation – were used "to quash rumours from misinformation, but also to counter disinformation" (Allison 2020; Telegraph Reports 2023). RRU and CDU deployment was consistent with governmental concern about "foreign interference" and disinformation disseminated by social media. Such matters are on the agenda of the Defending

Democracy Taskforce set up in December 2022 (Tugendhat 2022). The use of military expertise in support of government information policy certainly merits debate.

In June 2023, two influential conservative newspapers, *The Daily Telegraph* and its stablemate, *The Sunday Telegraph*, campaigned against regulation by take-down. They reported that the CDU was run by an ex-Home Office civil servant, Sarah Connolly, with a background in "anti-terror policy." Speculation about CDU connections with the intelligence services came amid claims that the unit made hourly calls to companies such as Facebook and Twitter (now X), flagging posts dissenting from Covid-19 policy (Investigations Team 2023a; 2023b). *The Telegraph*'s reports accused the RRU and CDU of working "with social media companies in an attempt to curtail discussion of controversial lockdown policies during the pandemic" (Investigations Team 2023c). An investigation by the Information Commissioner's Office into alleged secret monitoring of "online activities of prominent critics of the Government's covid policies" was reported (Investigations Team 2023d; 2023e).

To counter this narrative, the Cabinet Office and the Department of Science, Innovation and Technology (DSIT)(2023) issued a "fact sheet." The CDU, it maintained, was concerned with "risks to public health, public safety and national security." Since the Covid-19 emergency and the invasion of Ukraine by Russia in February 2022, 92 percent of referrals concerned "state backed disinformation." Presumably, 77 Brigade, unmentioned in the fact sheet, dealt with hostile Russian content. The RRU, a "digital cuttings service," had been "disbanded" (a curiously military term) in August 2022 and held no dossiers on journalists or politicians, although allegations made about files compiled on scientists and others were not countered. A government minister had previously said that "in some instances" the RRU "collected published material on organisations or individuals with a public profile" (Burghart 2023), leaving questions hanging about surveillance. This fusion of civil and military powers during a crisis combining national security and public health communications also merits public discussion.

The government employed regulatory methods – take-downs and monitoring content – to manage the scope of public debate, with clear implications for the workings of the political public sphere. However, it is not clear how effectively this was done. Although not officially secret, aspects of this activity verged on covert action subject to minimal public accountability. Although the Cabinet Office/DSIT factsheet declared that the RRU was "referenced" 16 times in Parliament, answers to MPs' questions were bland and evasive, citing national security and "the need to maintain good relations with platforms" as grounds for reticence (Trendall 2022, 3).

Notification as Regulation. Internet platform referrals have a venerable national predecessor. Established in 1912, the Defence or D-Notice system, was devised to influence the printed press on national security matters, amid intense pre-World War I concern about enemy propaganda and espionage. The investigative journalist, David Leigh (1980, 57), described it as "a line of advance censorship for the press on so-called national security matters." The whistle-blowing civil servant, Clive Ponting (1986, 147), acerbically called the system "a marvellous example of the 'good chaps' principle at work."

The state has used the D-Notice system to control freedom of expression in print journalism, broadcasting, and book publishing (Ewing and Gearty 1990; Michael 1982), provoking intermittent controversy. *Ex ante* guidance on what not to print (censorship by persuasion and occasionally by direction) long predates CTIRU's *ex post* extra-legal referrals for take-down. Leigh (1980, 58) thought the system was "sliding into graceful decline" during the 1980s. Instead, it modernised, acquiring a new face.

In 2015, following a review, the Defence and Security Media Advisory (DSMA) Committee was established. Notices once secret became public and extreme discretion was replaced by a website and published minutes. The Committee's role is to ensure "the security and well-being of the UK, its overseas territories and its citizens at home and abroad; and its system of government" (DSMA 2023).

"National security" is not defined by the DSMA but considered case by case according to "the threats facing, and the interests of, the UK and its allies." The DSMA Committee's government representatives come from key departments (foreign, home affairs, and defence). Continuing long-established practice, senior officials with national security remits meet representatives of the press and broadcasting, digital media, and industry bodies.

Cybersecurity and counterterrorism are on the DSMA's official agenda, as are intelligence operations, activities, and communication methods. Critical national infrastructure also comes within its purview. The DSMA Committee still focuses principally on traditional media. It engages with the main UK press regulator, the Independent Press Standards Organisation (IPSO) and has considered establishing an "arms-length" relationship with the media and communications regulator, Ofcom, "to influence the very largest digital platforms to ensure their algorithms do not *amplify* articles which may damage national security or increase the risk to people's lives" (DSMA 2022; original emphasis). Although DSMA notices have "no legal standing," their use raises questions about their chilling effect.

Overt and Covert Regulation. Official concern about national security matters is inscribed both in overt and covert regulatory processes. This is especially clear from concern about the impact on democracy of 'disinformation' and 'misinformation' from hostile actors, as well as content regulation related to counterterrorism. Both types of intervention seek to patrol the boundaries of the political public sphere by applying rules for what constitutes legitimate political discourse and actors. The defence of critical infrastructure is a further dimension of national security doctrine.

British statutory regulatory bodies are commonly accorded a certain autonomy. They are in the public domain, at the heart of the overt process and a focus of expert attention. However, as demonstrated, the executive culture of the covert regulatory process is strikingly different. Weak parliamentary accountability through ministers often leaves operational matters shrouded in secrecy on national security grounds. While we can distinguish between overt and covert modes of regulation, in practice these overlap where national security is concerned. Although the distinct forms of regulation occupy different clusters of positions in the regulatory field, these articulate with one another on the common ground of national security. The regulatory field will ramify further when firm rules of the game are established for AI, which is already high on the defence agenda.

Conclusion

The post-public sphere designates a structural transformation of uncertain duration and outcomes. As Habermas's latest work shows, the wholesale shift of content to the internet is perceived as a critical juncture for public sphere theory. In his latest foray, regulation has been promoted to the front line in addressing the shift from legacy media to platforms as well as the decline of widespread deliberation. What does this portend for the political public sphere in democracies? Habermas's rethinking of the new structural transformation of the public sphere conceives of regulation as a necessary tool for recreating conditions that begin to satisfy the normative requirements of his theory. However, the scope and scale of regulation and its conditions of existence remain almost entirely unexamined. This article has sought to explore that question in a variety of ways.

Regulatory responses by diverse states and the EU are rooted in geopolitical competition. In the present context of global rivalry, regulatory policy has foregrounded a major national security dimension, illustrated here by the British case. The UK's development of a complex regulatory field is applicable to other national contexts, giving due consideration to each polity's diverse legal, institutional, and administrative cultures and practices. How regulation works in practice

is an acid test for relations between state power and platform power. This requires us to think about the internal operations of the state as well as its external relations. So far as the former are concerned, this account has raised questions about how overt and covert regulation operate in a democracy that espouses national security doctrine. Beyond the level of the state, how new forms of global governance will develop under present conditions of geopolitical rivalry is also firmly on the agenda.

Although my account has illustrated how state power in the UK has responded to the digital challenge by way of neo-regulation, it has not addressed the efficacy of that response. That is a major issue for sustained research. So far as capitalist democracies are concerned, Robin Mansell (2023, 153) contends that dominant views of regulatory efficacy axiomatically assume that market economics will produce beneficial outcomes. The challenge is how to address the divergent pull between "corporate interests in monetising data for profit, state interests in data surveillance, and civil society interests in preserving their fundamental rights."

Regulatory clout depends on financial and expert resources possessed by agencies and their authority to obtain information and demand compliance. Executive interventions by states are part of the picture. The well-known risk of regulatory capture and how to address the revolving doors between regulators and platforms are on the agenda for research (Neudert 2023). Moreover, temporality plays a crucial role since regulatory capacity develops slowly relative to the rapid technological innovations in train. We now face the conundrum of how to articulate existing analysis of regulation with new challenges represented by AI.

Acknowledgements

I am grateful to the journal's reviewers and to Kris Erickson for their insightful comments.

Disclosure statement

No potential conflict of interest was reported by the author.

Funding

The research was supported by the AHRC Centre of Excellence for Policy & Evidence in the Creative Industries (PEC 1.0, 2018-23)(award reference no.: AH/S001298/).

References

Adamson, Fiona B. 2016. "Spaces of Global Security: Beyond Methodological Nationalism." *Journal of Global Security Studies* 1, no.1: 19–35. doi: 10.1093/jogss/ogv003.

Allison, George. 2020. "77 Brigade is Countering Covid Misinformation." *UK Defence Journal*, April 23, 2020. https://ukdefencejournal.org.uk/77-brigade-is-countering-covid-misinformation/#google_vignette.

Atkins, Victoria. 2019. "Answer to 'Radicalism: Social Media', Question for the Home Office." UK Parliament, July 8, 2019. https://questions-statements.parliament.uk/written-questions/detail/2019-06-26/269681.

Beck, Ulrich. 2006. *Cosmopolitan Vision*. Cambridge: Polity Press.

Bevir, Mark and Hall, Ian. 2014. "The Rise of Security Governance." In *Interpreting Global Security,* edited by Mark Bevir, Oliver Daddow, and Ian Hall, 17-34. Abingdon/New York: Routledge.

Boczkowski, Pablo J., and Zizi Papacharissi, eds. 2018. *Trump and the Media*. Cambridge MA.: The MIT Press.

Bok, Sissela. 1982. *Secrets: On the Ethics of Concealment and Revelation*. Oxford: Oxford University Press.

Boltanski, Luc, and Chiapello, Eve. 2005 [1999]. *The New Spirit of Capitalism*. Translated by Gregory Elliott. London: Verso.

Bourdieu, Pierre. 1986 [1979]. *Distinction: A Social Critique of the Judgement of Taste*. Translated by Richard Nice. London: Rouletdge & Kegan Paul Ltd.

Bourdieu, Pierre. 1993 [1968-87]. *The Field of Cultural Production*. Edited and introduced by Randal Johnson. Cambridge: Polity Press.

Bourdieu, Pierre. 1996 [1989]. *The State Nobility: Elite Schools in the Field of Power.* Translated by Lauretta C. Clough. Cambridge: Polity Press.

Braithwaite, John, and Drahos, Peter. 2000. *Global Business Regulation*. Cambridge: Cambridge University Press.

Burghart, Alex. 2023. "Rapid Response Unit, Question for Cabinet Office." UK Parliament, February 20, 2023. https://questions-statements.parliament.uk/written-questions/detail/2023-02-20/148802.

Cabinet Office and Department for Digital, Culture, Media and Sport. 2020. "Government Cracks Down on Spread of False Coronavirus Information Online." Press Release, March 30, 2020. https://www.gov.uk/government/news/government-cracks-down-on-spread-of-false-coronavirus-information-online.

Cabinet Office and Department for Science Innovation and Technology. 2023. "Government Response: Fact Sheet on the CDU and RRU. Fact Sheet on the Work of the Government's Counter-Disinformation Unit and Rapid Response Unit." June 9, 2023. https://www.gov.uk/government/news/fact-sheet-on-the-cdu-and-rru.

Cabinet Office and National Cyber Security Centre (NCSC). 2021. *Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report 2021*. July 20, 2021. https://www.gov.uk/government/publications/huawei-cyber-security-evaluation-centre-hcsec-oversight-board-annual-report-2021.

Calabrese, Andrew, and Robin Mansell. 2023. "The MacBride Report: Critical Scholarship and the Report's Value to Future Generations." In *Reflections on the International Association for Media and Communication Research: Many Voices, One Forum*, edited by Jörg Becker and Robin Mansell, 211-19. London: Palgrave Macmillan.

Chadwick, Andrew. 2017. *The Hybrid Media System: Politics and Power*. Oxford: Oxford University Press.

Chakravartty, Paula and Katharine Sarikakis. 2006. *Media Policy and Globalization*. Edinburgh: Edinburgh University Press.

CMA. 2020. Overview of the CMA's Provisional Approach to Implement the New Digital markets Competition Regime. Competition and Markets Authority. January 2024. https://assets.publishing.service.gov.uk/media/659ee36de8f5ec000d1f8b60/20240110_overview_of_digital_markets_regime_-_FINAL_for_publication.pdf

Cohen, Julie E. 2016. "The Regulatory State in the Information Age." *Theoretical Inquiries in Law* 17(2): 369-414. https://scholarship.law.georgetown.edu/cgi/viewcontent.cgi?article=3552&context=facpub.

Criddle, Cristina. 2024. "Ofcom Poaches Big Tech Staff in Push to Enforce New Internet Curbs." *Financial Times*, January 9, 2024. https://www.ft.com/content/19e9da57-5da4-40bc-989d-9820bf3d2aff.

Crouch, Colin. 2004. *Post-Democracy*. Cambridge: Polity Press.

Crouch Colin. 2019. "Post-Democracy and Populism." *The Political Quarterly* 90 (1): 124-137. https://doi.org/10.1111/1467-923X-12638

D'Ancona, Matthew. 2017. *Post-Truth: The New War on Truth and How to Fight Back*. London: Ebury Press.

Daniels, Mario and John Krige. 2022. *Knowledge Regulation and National Security in Postwar America*. Chicago: The University of Chicago Press.

Davis, Aeron. 2019. *Political Communication: A New Introduction for Crisis Times.* Cambridge: Polity Press.

Department for Digital, Culture, Media & Sport (DCMS). 2022. "UK Digital Strategy. Policy Paper." Updated October 4, 2022. https://www.gov.uk/government/publications/uks-digital-strategy/uk-digital-strategy.

Department for Science, Innovation & Technology, Foreign, Commonwealth & Development Office, Prime Minister's Office. 2023. "The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023." November 1, 2023. https://www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023.

Department of Commerce. 2023."At the Direction of President Biden, Department of Commerce to Establish U.S. Artificial Intelligence Safety Institute to Lead Efforts on AI Safety." Press Release, November 1, 2023. https://www.commerce.gov/news/press-releases/2023/11/direction-president-biden-department-commerce-establish-us-artificial.

Digital Competition Expert Panel (DCEP). 2019. *Unlocking digital competition*. HM Treasury and BEIS. https:// www.gov.uk/government/publications/unlocking-digital-competition-report-of-the-digital-competition-expert- panel.

Digital Regulators Cooperation Forum (DRCF). 2021. "Embedding coherence and cooperation in the fabric of digital regulators. CMA, Ofcom and ICO." https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/982898/DRCF_response_to_DCMS__PDF.pdf.

Dinenage, Caroline. 2020. "Letter from the Minister for Digital and Culture to Lord Puttnam, Chair of the House of Lords Democracy and Digital Technologies Committee, Regarding the Counter-

Disinformation Unit." Department for Digital, Culture, Media & Sport, INT2020/08 108/DC, May 29, 2020,

Downs, Anthony. 1972. "Up and Down with Ecology: The 'Issue-attention cycle'." *Public Interest*, 28 (Summer): 38–51. https://www.nationalaffairs.com/public_interest/detail/up-and-down-with-ecologythe-issue-attention-cycle.

DSMA. 2022. "Minutes of a Meeting held in the Ministry of Defence at 6pm on Thursday, May 12, 2022." Defence and Security Media Advisory Committee. https://www.dsma.uk/news.

DSMA. 2023. "The DSMA Notice System." Defence and Security Media Advisory Committee. https://www.dsma.uk.

Dunne, Niamh. 2021. "Concurrency." *The UK Competition Regime: A Twenty-year Retrospective,* edited by Barry Rodger, Peter Whelan, and Angus McCulloch, 255–81. Oxford Academic. https://doi.org/10.1093/oso/9780198868026.003.0010.

Eghbariah, Rabea, and Amre Metwally. 2021. "Informal Governance: Internet Referral Units and the Rise of State Interpretations of Terms of Service." *Yale Journal of Law and Technology* 23 (Spring): 542-616. https://yjolt.org/informal-governance-internet-referral-units-and-rise-state-interpretation-terms-service.

Emirbayer, Mustafa, and Victoria Johnson. 2018. "Bourdieu and organizational analysis." *Theory and Society,* 37, no.1(January): 1–44. https://doi.org/10.1007/s11186-007-9052-y.

Engler, Alex. 2023. "The EU and U.S. Diverge on AI Regulation: A Transatlantic Comparison and Steps to Alignment." Brookings, Center for Technology Innovation. April 25, 2023. https://www.brookings.edu/articles/the-eu-and-us-diverge-on-ai-regulation-a-transatlantic-comparison-and-steps-to-alignment/.

Ewing, Keith D., and Conor A. Gearty. 1990*. Freedom under Thatcher: Civil Liberties in Modern Britain*. Oxford: Clarendon Press.

Faroohar, Rana. 2023. "US Antitrust has Reached a Turning Point." Financial Times, October 9, 2023. https://www.ft.com/content/6c550fd5-9a4a-45d1-a457-296c0a52e192.

Flew, Terry. 2021. *Regulating Platforms*. Cambridge: Polity Press.

Flew, Terry. 2024. "The Return of the Regulatory State: Nation-States as Policy Actors in Digital Platform Governmance." In *Global Communication Governance at the Crossroads*, edited by Claudia Padovani, Véronique Wavre, Arne Hintz, Gerard Goggin, and Petros Iosifides, 161-78. London: Palgrave MacMillan. https://doi.org/10.1007/978-3-031-29616-1_12.

Fossum, John Erik and Philip Schlesinger, eds. 2007. *The European Union and the Public Sphere: A Communicative Space in the Making?* London/New York Routledge.

Garnham, Nicholas. 1994. "The Media and the Public Sphere." In *Habermas and the Public Sphere*, 359-76, edited by Craig Calhoun, Cambridge, MA: The MIT Press.

Golding, Peter, and Phil Harris, eds.1997. *Beyond Cultural Imperialism: Globalization, Communication and the New International Order*. London: SAGE Publications.

Government Information Service (GIS). 2018. "Alex Aitken Introduces the Rapid Response Unit." News, July 19, 2018. Archived, The National Archives, February3, 2020. https://webarchive.nationalarchives.gov.uk/ukgwa/20200203104056/https:/gcs.civilservice.gov.uk/news/alex-aiken-introduces-the-rapid-response-unit/.

Gripsrud, Jostein and Hallvard Moe. 2010. "Introduction," In *The Digital Public Sphere: Challenges for Media Policy,* edited by Jostein Gripsrud and Hallvard Moe, 9–19. Göteborg: Nordicom.

Habermas, Jürgen. 1989 [1962]. *The Structural Transformation of the Public Sphere: An Inquiry into a Category of Bourgeois Society*. Translated by Thomas Burger with the assistance of Frederick Lawrence. Cambridge: Polity Press.

Habermas, Jürgen. 1996 [1992]. *Between Facts and Norms: Contributions to a Discourse Theory of Law and Democracy*. Translated by William Rehg. Cambridge: Polity Press.

Habermas, Jürgen. 2009 [2008]. "Political Communication in Media Society: Does Democracy still Have an Epistemic Dimension? The Impact of Normative Theory on Empirical Research." In Jürgen Habermas, *Europe: the Faltering Project*, 138-183. Translated by Ciaran Cronin. Cambridge: Polity Press.

Habermas, Jürgen. 2023 [2018-2022]. *A New Structural Transformation of the Public Sphere and Deliberative Politics*. Translated by Ciaran Cronin. Cambridge: Polity Press.

Harvey, David. 2005. *A Brief History of Neoliberalism*. Oxford: Oxford University Press.

Hayes, John. 2023. "Answer to 'Counter-terrorism', Question for the Home Office." UK Parliament, March 17, 2016. https://questions-statements.parliament.uk/written-questions/detail/2016-03-14/30894.

HCSEC. 2020. "Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board. Annual Report 2020." A Report to the National Security Adviser of the United Kingdom. September, 2020.

Helberger, Natali. 2020. "The Political Power of Platforms: How Current Attempts to Regulate Misinformation Amplify Opinion Power." 2020. *Digital Journalism* 8, no. 6: 842-54. https://doi.org/10.1080/21670811.2020.1773888.

HM Government. 2021. *Global Britain in a Competitive Age: The Integrated Review of Security, Defence, Development and Foreign Policy* CP403, March 2021. https://www.gov.uk/government/publications/global-britain-in-a-competitive-age-the-integrated-review-of-security-defence-development-and-foreign-policy/.

HM Government. 2023. *Integrated Review Refresh: Responding to a More Contested and Volatile World*. Presented to Parliament by the Prime Minister by Command of His Majesty, CP811, March 2023. https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1145586/11857435_NS_IR_Refresh_2023_Supply_AllPages_Revision_7_WEB_PDF.pdf.

Investigations Team. 2023a. "Exclusive: Ministers Had a 'Chilling' Secret Unit to Curb Lockdown Dissent." *The Daily Telegraph*, June 2, 2023.

Investigations Team. 2023b. "Monitoring Unit Made Hourly Calls to Flag Covid Dissent." *The Daily Telegraph*, June 10, 2023.

Investigations Team. 2023c. "Twitter Turned Down Half of CU Requests for Censorship." *The Sunday Telegraph*, June 11, 2023.

Investigations Team. 2023d. "Covid Unit 'Broke its Own Rules'." *The Daily Telegraph*, June 12, 2023.

Investigations Team. 2023e. "Watchdog Tackles Covid Disinformation Unit." *The Daily Telegraph*, June 13, 2023.

Keane, John. 1991. *The Media and Democracy*. Cambridge: Polity Press.

Kretschmer, Martin, Ula Furgał, and Philip Schlesinger. 2022. "The Emergence of Platform Regulation in the UK: An Empirical-Legal Study." *Weizenbaum Journal of the Digital Society* 2, no.2: 12-31. https://doi.org/10.34669/wi.wjds/2.2.4.

Larkin, Brian. 2013. "The Politics and Poetics of Infrastructure." *Annual Review of Anthropology* 42: 327-343. http://doi.org/10.1146/annurev-anthro-092412-155522.

Leigh, David. 1980. *The Frontiers of Secrecy: Closed Government in Britain*. London: Junction Books.

Levi-Faur, David, Yael Kariv-Teitelbaum, and Rotem Medzini. 2021. "Regulatory Governance: History, Theories, Strategies Yael and Challenges." *Oxford Research Encyclopedia of Politics*. https://doi.org/10.1093/acrefore/9780190228637.013.1430.

Livingstone, Sonia, and Peter Lunt. 2013. "Media Studies' Fascination with the Concept of the Public Sphere: Critical Reflections and Emerging Debates." *Media, Culture & Society* 35(1): 87-96. https://doi.org/10.1177/0163443712464562.

MacBride, Séan. 1980. *Many Voices, One World*. London: Kogan Page.

Mancini, Paolo. 2023. "Features of the Digital Era: Deinstitutionalisation and Reinstitutionalisation." In *Streamlining Political Communication Concepts: Updates, Changes, Normalcies*, edited by Susana Salgado and Stylianos Papathanassopoulos, 13-22. London: Palgrave Macmillan.

Mansell, Robin. 2023. "Digital Technology Innovation: Mythical Claims about Regulatory Efficacy". *Javnost - The Public* 30(2):145-160. https://doi.org: 10.1080/13183222.2023.2198933.

Mattelart, Armand. 1979 [1976]. *Multinational Corporations and the Control of Culture: The Ideological Apparatuses of Imperialism*. Translated by Michael Chanan. Brighton: The Harvester Press.

Mattelart, Armand and Michelle, Mattelart. 1992 [1986]. *Rethinking Media Theory: Signposts and New Directions*. Translated by James A. Cohen and Marina Urquidi. Minneapolis: University of Minnesota Press.

Michael, James. 1982. *The Politics of Secrecy: Confidential Government and the Public Right to Know*. Harmondsworth: Penguin Books Ltd.

Mihelj, Sabina. 2023. "Platform Nations." *Nations and Nationalism* 29(1): 10-24. http://doi.org/10.1111/nana.12912.

Miller, Chris. 2022. *Chip War: The Fight for the World's Most Critical Technology*. London: Simon & Schuster.

Moran, Michael. 2004. *The British Regulatory State: High Modernism and Hyper-innovation.* Oxford: Oxford Academic. https://doi.org/10.1093/0199247579.001.0001.

Mueller, Milton. 2017. *Will the Internet Fragment? Sovereignty, Globalization, and Cyberspace*. Cambridge: Polity Press.

National Audit Office (NAO). 2023. "Preparedness for Online Safety Regulation." https://www.nao.org.uk/reports/preparedness-for-online-safety-regulation/.

Neudert, Lisa-Maria. 2023. "Regulatory Capacity Capture: The United Kingdom's Online Safety Regime." *Internet Policy Review* 12(4): 2-34. https://doi.org/10.14763/2023.4.1730.

Nieminen, Hannu, Claudia Padovani, and Helena Sousa. 2023. "Why Has the EU Been Late in Regulating Social Media Platforms? *Javnost – The Public* 30(2): 174–196. https://doi.org/10.1080/13183222.2023.2200717.

O'Hara, Ciaran, and Hall, Wendy. 2021. *Four Internets: Data, Geopolitics, and the Governance of Cyberspace*. New York: Oxford University Press.

Open Rights Group. 2023. "Counter-Terrorism Internet Referral Unit." https://wiki.openrightsgroup.org/wiki/Counter-Terrorism_Internet_Referral_Unit.

Plantin, Jean-Christophe, and Aswin Punathambekar. 2019. "Digital Media Infrastructures: Pipes, Platforms and Policies." *Media, Culture & Society* 41(2): 163-174. https://doi.org/10.1177/0163443718818376.

Ponting, Clive. 1986. *Whitehall: Tragedy and Farce*. London: Sphere Books Ltd.

Rantanen, Terhi. 2017. "'Crisscrossing' Historical Analysis of Four Theories of the Press." *International Journal of Communication* 11: 3454-475.

Reuters Institute for Journalism. 2023. *Digital News Report 2023.* https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2023-06/Digital_News_Report_2023.pdf.

Runciman, David. 2018. *How Democracy Ends*. London: Profile Books.

Sapiro, Gisèle. 2018. "Field Theory from a Transnational Perspective." In *The Oxford Handbook of Pierre Bourdieu*, edited by Thomas Medvetz and Jeffrey J. Sallaz, 161-82. Oxford: Oxford Academic. https://doi.org/10.1093/oxfordhb/9780199357192.013.7.

Schlesinger, Philip. 1991. *Media, State and Nation: Political Violence and Collective Identities*. London: SAGE Publications Ltd.

Schlesinger, Philip. 2015. "Transnational Framings of British Film Policy." In *Transnational Mediations: Negotiating Popular Culture between Europe and the United States*, edited by Christof Decker and Astrid Böger, 191-208. Heidelberg: Universitätsverlag Winter.

Schlesinger, Philip. 2020. "After the Post-Public Sphere." *Media, Culture & Society*, 42, nos.7-8 (October-November): 1545–1563. https://doi.org/10.1177/0163443720948003.

Schlesinger, Philip. 2022. "The Neo-Regulation of Internet Platforms in the United Kingdom." *Policy & Internet* 14(1): 47–67. https://doi.org/10.1002/poi3.288.

Sheehan, Matt. 2023. *China's AI Regulations and How they Get Made*. Working Paper. Carnegie Endowment for International Peace. July 2023. https://carnegieendowment.org/2023/07/10/china-s-ai-regulations-and-how-they-get-made-pub-90117.

Shepley, Paul and Matthew Gill. 2023. "Artificial Intelligence: How is the Government Approaching Regulation?" Explainer, Institute of Government, October 27, 2023. https://www.instituteforgovernment.org.uk/explainer/artificial-intelligence-regulation.

Siebert, Fredrick S., Theodore Peterson, and Wilbur Schramm. 1956. *Four Theories of the Press*. Urbana IL: University of Illinois Press.

Splichal, Slavko. 2022. "The Public Sphere in the Twilight Zone of Publicness." *European Journal of Communication* 37, (2): 198-215. https://doi.org/10.1177/02673231211061490.

Springer, Simon. 2016. *The Discourse of Neoliberalism: An Anatomy of a Powerful Idea*. London/ New York: Rowan & Littlefield International.

Street, John. 2001. *Mass Media, Politics and Democracy*. Basingstoke: Palgrave.

Telegraph Reports. 2023. "Army's 'Information Warfare'" Unit Monitored Covid Lockdown critics." *The Daily Telegraph*, January 29, 2023.

Thomas, Huw. 2022. "Chinese Ownership of Newport Microchip Plant a 'Security Risk'." BBC News. https://www.bbc.co.uk/news/uk-wales-63656816.

Trappel, Josef, Leen d'Haenens, Hannu Nimenen, and Barbara Thomas. 2024. "Policy Responses to Digital Communication Platforms with a Focus on Europe." In *Global Communication Governance at the Crossroads*, edited by Claudia Padovani, Véronique Wavre, Arne Hintz, Gerard Goggin, and Petros Iosifides, 199-216. London: Palgrave MacMillan. https://doi.org/10.1007/978-3-031-29616-1_12.

Trendall, Sam. 2022. "Wall of Secrecy Surrounds DCMS's Counter-Disinformation Unit." *Civil Service World*, February 22, 2022. https://www.civilserviceworld.com/professions/knowledge-information-management.htm.

Tugendhat, Tom. 2022. "Defending Democracy in an Era of State Threats." Speech by the Security Minister, Home Office, delivered to the Policy Exchange, December 13, 2022. https://www.gov.uk/government/speeches/defending-democracy-in-an-era-of-state-threats.

UK Public General Acts. 2023. *Online Safety Act 2023*. October 26, 2023. https://www.legislation.gov.uk/ukpga/2023/50/enacted.

Van Dijck, José, Thomas Poell, and Martijn De Waal. *The Platform Society: Public Values in a Connective World*. Oxford: Oxford University Press.

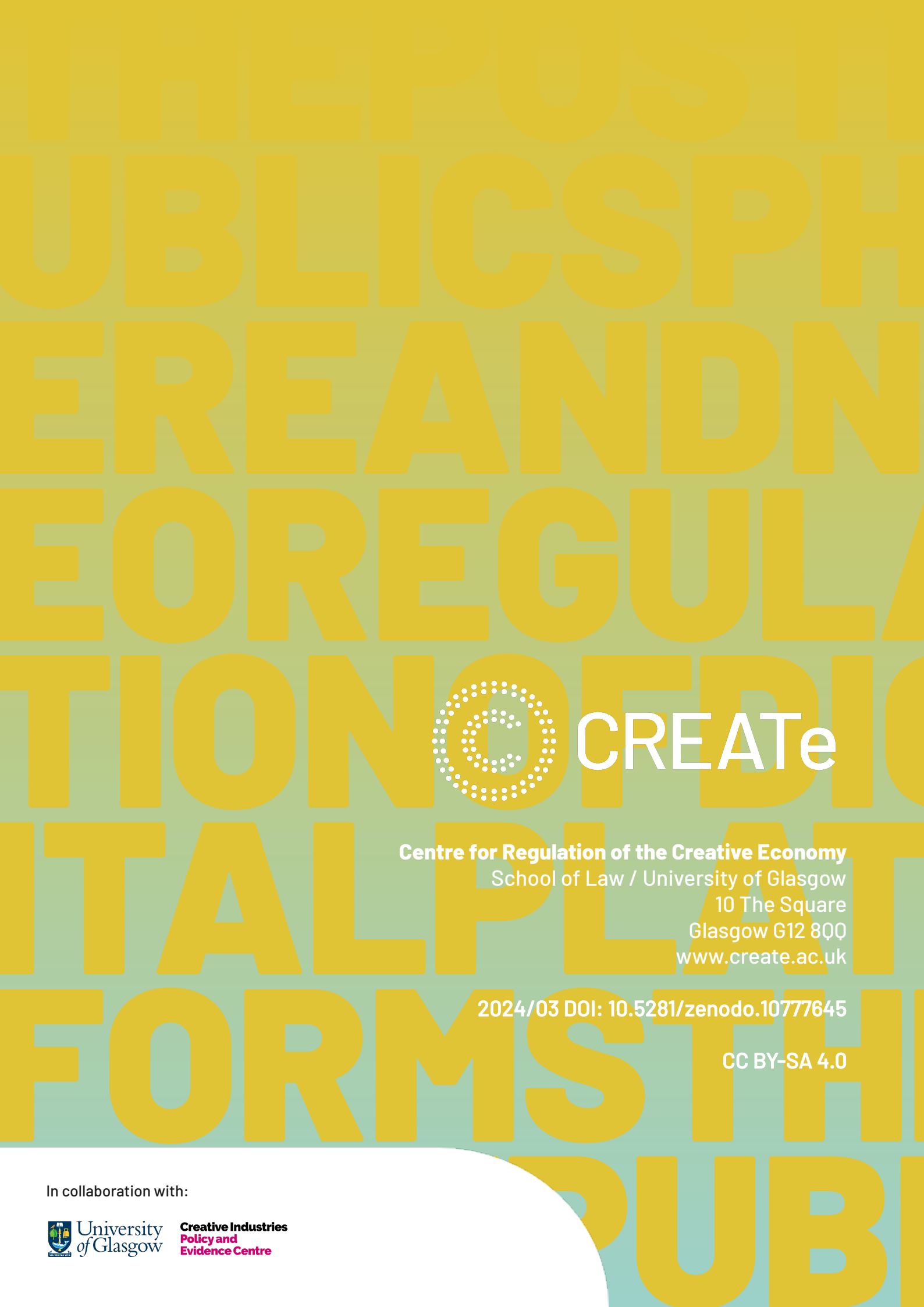
Vanberg, Aysem Diker. 2023. "Cordinating Digital Regulation in the UK: Is the Digital Regulation Cooperation Forum (DRCF) up to the Task?" *International Review of Law, Computers and Technology* 37, no.2 (March): 128-146. https://doi.org/10.1080/13600869.2023.2192566.

Wacquant, Loïc J. D. 1996. "Foreword" to Pierre Bourdieu, In *The State Nobility*, ix-xxii. Cambridge: Polity Press.

Wodak, Ruth, and Michał Krzyzanowski, eds. 2017. "Right Wing Populism in Europe and USA: Contesting Politics and Discourse beyond 'Orbanism' and 'Trumpism'." *Journal of Language and Politics* 16(4): 471-484.

WSIS. 2005. *World Summit on the Information Society, Outcome Documents, Geneva 2003-Tunis 2005.* World Summit on the Information Society, United Nations, International Telecommunication Union. https://www.itu.int/net/wsis/documents/doc_multi.asp?lang=en&id=2316|0.

Zuboff, Shoshana. 2019. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. London: Profile Books.



Centre for Regulation of the Creative Economy
School of Law / University of Glasgow
10 The Square
Glasgow G12 8QQ
www.create.ac.uk

2024/03 DOI: 10.5281/zenodo.10777645

In collaboration with:

University of Glasgow

Creative Industries Policy and Evidence Centre