INTERNET POLICY REVIEW
Journal on internet regulation

Volume 12 **Issue** 4

RESEARCH ARTICLE

OPEN ACCESS

PEER REVIEWED

Regulatory capacity capture: The United Kingdom's online safety regime

Lisa-Maria Neudert *University of Oxford*

DOI: https://doi.org/10.14763/2023.4.1730

Published: 1 December 2023
Received: 9 December 2022 **Accepted:** 17 July 2023

Competing Interests: The author has declared that no competing interests exist that have influenced the text.

Citation: Neudert, L.-M. (2023). Regulatory capacity capture: The United Kingdom's online safety regime. *Internet Policy Review*, *12*(4). https://doi.org/10.14763/2023.4.1730

Keywords: Platform regulation, Platforms, United Kingdom, Online safety, Regulatory capacity

Abstract: Worldwide, governments are increasingly concerned about the spread of online harms and big tech's apparent inability to effectively curb them. While some democracies have swiftly implemented regulatory reforms, others, including the United Kingdom, have encountered challenges in developing regulations aimed at platforms. This research investigates the development of the UK's Online Safety Act (OSA) as a key case to examine government capacity for regulating digital platforms. It explores the dynamics between the UK government and platforms, revealing persistent resource asymmetries that not only challenge the government's capacity to regulate but also significantly impact the development of regulatory policies. Drawing from empirical evidence from 33 in-depth, elite interviews with stakeholders from government, industry, and civil society, and archival review, the paper proposes an original framework of regulatory capacity consisting of four resources: information, treasure, authority, and organised expertise. The study finds: 1) the government lacks fundamental regulatory capacity, impeding the development of effective platform regulation; 2) platforms hold superior resources for countering online safety issues; 3) capacity asymmetries between government and platforms pose sustained risks for regulatory capture. Bringing these findings into context with the OSA, this research contends that the Act empowers the government to effectively utilise platform resources for regulatory purposes. However, the success of the Act hinges on the government's capacity to use its authority and enforce the online safety regime. Moving forward, the capacity-based approach introduced in this research offers a rich, analytical framework to examine how the complex interplay between actors and resources affects emergent regulatory systems, thus guiding the development of more robust regulatory strategies.

Introduction

Internet platforms are integral to contemporary public life. A handful of big tech corporations have emerged as central conduits of economic, social and political activity. Unparalleled in size and valuation, these digital platforms provide access to information, foster democratic mobilisation, drive economic growth and connect billions of users to each other every day (Chadwick, 2013; Howard & Hussain, 2013; Margetts et al., 2016). Yet as internet services become ubiquitous, concerns about their impact mount. A growing body of research reveals that platforms are host to a variety of online harms. They amplify nefarious content, harvest sensitive user data, abuse their market power to stifle competition, profit from foreign information operations, promote polarisation and enable oppressive surveillance – putting their users' online safety at risk (Au et al., 2021; Chan & Kwok, 2021; Howard, 2020; Zuboff, 2019).

Governments worldwide have grown concerned about pressing platform problems and big tech's inability to solve them. Since 2016, at least 100 governments – among them countries like Australia, France, Germany, Spain, Singapore and South Korea, and notably the European Union – have implemented regulations aimed at safeguarding against online harms on internet platforms. Emergent regulatory measures aim at creating a safer digital space and often span an array of policy issues, including content controls, antitrust and data protection (Bradshaw et al., 2018; Yadav et al., 2021).

In the United Kingdom (UK), the development of platform regulation has been fraught with significant delays, despite early initiatives and sustained public demand for internet protections. Proposals for a platform-aimed regulatory regime, the Online Safety Bill (OSB), were first put forward in 2017, positioning the UK an early proponent of platform regulation. Yet, despite sustained political support for such regulations – which persisted through the Covid-19 pandemic and several government leadership crises – the progression of the bill was repeatedly stalled. It was not until October 2023, that the OSB was enacted and is now referred to as the Online Safety Act (OSA). Given the government's early advocacy and continuous administrative efforts, why has the United Kingdom faced such challenges in developing platform regulation?

Against the backdrop of the newly adopted online safety regime, I use the UK as a case study to analyse systemic issues underpinning the development platform regulation. I offer evaluative, explanatory, and normative perspectives to enable the analysis of an emergent regulatory landscape. Looking beyond existing work on

challenges obstructing regulation, I shift attention towards capacity for the regulation of platforms to explain regulatory development. My research questions are:

RQ1 How does the regulatory capacity of state actors compare to that of platform actors in developing platform-focused regulations, specifically considering the resources available to each?

RQ2 How do the capacity constellations of state and platform actors, as well as their interplay with regard to resources, shape the development of regulation within an emergent regulatory system?

RQ3 What regulatory measures – considering in particular those outlined in the Online Safety Act – are required to address capacity challenges in the regulation of online platforms, and how likely are they to be effective in achieving the intended regulatory goals?

To answer these questions, the article proceeds as follows. I begin by offering a review of scholarly literature on platform regulation and regulatory capacity. Bringing these bodies of research into dialogue to identify the key challenges to platform regulation, I develop an original framework of four regulatory resources – information, treasure, authority, and organised expertise – that are essential for building regulatory capacity in this space. This is followed by a methods section, detailing the way in which the evidence from 33 elite interviews with participants in government, industry and civil society is analysed and supplemented by archival analysis. Employing the original framework of regulatory capacity to the empirical study of platform regulation, I draw from interview evidence and regulatory theory to analyse state-platform interplay in regulatory development in the UK. Based on the interview evidence and regulatory theory, I employ the original framework of regulatory capacity to the empirical study of platform regulation development in state-platform interplay in the UK, contributing to the development of this research area. I find that: 1) government lacks essential regulatory resources, frustrating its capacity as a regulator; 2) platforms hold resource advantages over government resulting in capacity asymmetries; and 3) asymmetric resource constellations give rise to regulatory capture whereby platforms leverage resources for influence over regulation. The discussion examines the regulatory measures necessary to address capacity asymmetries in platform regulation, with a specific focus on the measures in the UK's Online Safety Act and their potential to overcome capacity challenges.

Moving forward, the capacity-based approach developed here provides a unique

analytical framework for understanding challenges to regulatory developments. By identifying these challenges as a resource-based interplay between the state and platforms, this approach offers decisional insights into the feasibility and strategies of overcoming capacity asymmetries and risks of capture.

Platform regulation: challenges, capacity and capture

Challenges to regulation

As governments worldwide pursue online safety regulation, a growing body of literature is devoted to the study of emergent regulatory measures, often captured under the umbrella term "platform regulation". This literature commonly revolves around challenges to regulation, which are described as 'hurdles', 'obstacles' or 'barriers' that states must overcome to pursue regulation (Flew & Gillett, 2021; Hoffmann-Riem, 2020; Taeihagh et al., 2021). Drawing from and distilling the existing literature, I identify three fundamental types of challenges to platform regulation – technical, institutional, and political challenges – that are commonly discussed in the discourse on online safety regulation. By examining evidence from the UK, I offer an analytical lens to explore the impact of these challenges on the development of platform regulation, both in the UK and beyond.

Scholarship on technical challenges postulates that digital technologies pose a fundamental barrier to established regulatory practice. This line of inquiry argues that existing regulatory tools prove ill-equipped for the regulation of complex technical features (Gorwa et al., 2020; Neudert, 2020). This challenge is widely acknowledged in the UK context. For example, the Department for Digital, Culture, Media and Sport (DCMS) argues that "distinctive features which make digital businesses and applications unique" (DCMS, 2022a, Context section) make necessary a "distinct regulatory approach" to be set out in original regulation (DCMS, 2022a, Context section; also quoted in Dommett & Zhu, 2022, p. 3).

Institutional challenges focus on barriers connected to regulatory frameworks with regards to their suitability for platform regulation. This research details challenges around regulatory remits that are not fit for purpose, gaps in legislation, and unintended or otherwise undesirable policy outcomes (Schlesinger, 2022; Woods, 2019). In the context of the UK's pending online safety regime, experts have raised concerns over stifling effects on civic freedoms in connection to provisions for the removal of 'harmful but legal speech' – speech that is legal offline but that could be subject to intervention online (Coe, 2022; Dittel, 2022; Trengove et al., 2022). Meanwhile, Neudert (2020) argues that platforms escaped regulatory oversight

around the Cambridge Analytica scandal because of unclear regulatory mandates in the UK at the time (Wylie, 2019).

Thirdly, political challenges emphasise “processes through which the domestic regulatory activities of states and other actors set effective rules” (Farrell & Newman, 2010, p. 1). Tracing regulatory processes, scholars show that factors like electoral considerations, regulatory activism pursued by influential politicians and logistical constraints, for example around parliamentary schedules, impact platform regulation (Flew et al., 2021; Gorwa, 2021). In the UK context, Dommett and Zhu (2022) find that policymakers have struggled to harmonise and find consensus around conflicting policy proposals for an online safety regime, and this has caused delays. Experts have also connected delays to Covid-19 and the 2022 government leadership crisis and, coming along with it, constant turnover in the position of the DCMS Secretary of State (Hern, 2022; Kent et al., 2020). Furthermore, the proposals surrounding "legal but harmful" content and encryption became contentious issues. Tech firms, along with free speech and privacy organisations, strongly opposed the government's stance, resulting in sustained debate (Scott & Dickson, 2023).

Regulatory capacity

The body of research discussed above highlights persistent problems faced by state regulators in developing regulation but has not dealt with questions as to why challenges exist and how they can be overcome in interplay with platform regulatees. Therefore, I argue that there is value in shifting perspective away from challenges impeding regulation - that is a focus on non-regulation - and towards regulatory capacity enabling regulation – that is a focus on regulation. To facilitate this analytical focus, I propose an original four-part framework of regulatory capacity that entwines theoretical notions of regulatory resources and the tools of government (Black, 2002, 2003; Hood, 1983). In my conception of regulatory capacity, I draw from Julia Black:

“Regulatory capacity is the actual or potential possession of resources plus the existence of actual or potential conditions that make it likely that those resources will be deployed both now and in the future in such a way as to further the identified goals of the regulatory system or resolve identified problems”. (Black, 2003, p. 68)

Black presents an actor- and resource-centric understanding of regulation. According to Black, an actor’s capacity to regulate is directly related to its ability to de-

ploy relevant resources. She applies this framework to both the development and implementation of regulation and argues that it can be used to inform regulatory practice. Black contends that regulation requires different resources, whereby some actors have superior capacity to others, depending on their relative resource configuration. She further argues that resource constellations that should inform how regulatory functions "are and should be distributed between diverse actors in a regulatory system" (Black, 2003, p. 63). In this context, regulators can overcome capacity deficits by collaborating with other actors that possess different resource configuration leveraging asymmetries in resources for regulation (Black, 2003, p. 74).

In Black's work on regulatory capacity, she develops a model of six resources – information, expertise, financial resources, authority and legitimacy, strategic position, and organisational capacity – that state and other actors, such as a regulated firm or a third-party body, can enrol in regulation. However, the model lacks conceptual clarity and the six resources intersect[1]. Black draws heavily from Hood's "tools of government" (Hood, 1983) approach which postulates that there are four tools – nodality (the property of being in the middle of a network), authority, treasure, and organisation – that governments use to govern. Furthermore, the "tools-based approach" (Hood, 1983) suggests that the government occupies a position "above other actors and can unilaterally select instruments and deploy them" (Black, 2003, p. 1).

Based on the interaction between these theories on regulatory resources, the synthesis of empirical evidence collected for this research, and taking into account Hood's and Margetts' (2007) work on the tools of government in a digital age, I propose a modified *capacity-based* framework that distils four resources that are relevant for platform regulation and become deployed by hybrid actors: information, treasure, authority, and organised expertise (Table 1). This framework offers a contemporary understanding of regulation that recognises the regulatory capacity of both state and non-state actors, challenging traditional notions of regulation that solely focus on the state (contra Hood, 1983). What is more, the approach goes beyond binary notions of the possession or non-possession of resources, and instead examines resource configurations and an actor's ability to use them for platform regulation including in collaboration with other actors. Finally, building upon Black, I posit that the framework can be used to study both the development

1. For example, Black's conception of financial resources as a resource provides that financial resources are "largely instrumental" whereby the possession of financial resources enables the possession of other regulatory resources. However, according financial resources themselves are not directly deployed towards regulatory functions (see Black, 2002, 2003).

of regulation and its implementation, providing insights on capacity-based challenges and solutions to questions around platform regulation.

The proposed framework of regulatory capacity aligns with emergent theory on the regulation of digital platforms, which emphasises the role of hybrid regulation spanning interconnected regulatory actors and the enrollment of their respective resources in regulation (Levi-Faur, 2011). Theoretical conceptions of platform regulation commonly recognise the involvement of multiple actors in platform regulation, spanning the regulation "of and by platforms" (DeNardis & Hackl, 2015; Gillespie, 2018, p. 254) or even "multi-actor governance structures" (Papaevangelou, 2021).

Yet existing empirical work on the subject tends to focus on either state-led hierarchical or corporate-led self-regulatory systems, with little attention paid to hybrid state and platform actors and their relative resources in interplay. Scholars of hierarchical regulation argue that platforms are subject to superordinate state authority in state-led regulatory systems (Barrett et al., 2021; Theil, 2019; Woods, 2019). Conversely, research on platform-led self-regulation commonly maintains that platform actors have emerged as potent "new governors" (Klonick, 2017) that supersede state power (Gorwa, 2019; Suzor, 2019).

Using a capacity-based approach to the study of regulatory development, this research expands on existing theory and shifts the focus to the study of the interplay between hybrid state and platform actors and their relative resources to trace how they are enrolled in emergent platform regulation. By studying the configurations of resources of state and platform actors in interplay, this approach reveals resource deficits and relative asymmetries, offering new insights into the underlying actor relationships of platform regulation.

Regulatory capture

To reflect on the impact of resource asymmetries on regulation, I bring the framework of regulatory capacity into dialogue with theories of regulatory capture. On a basic level, regulatory capture occurs when a regulator becomes co-opted by the interests of the regulatee or another third party (Dal Bó, 2006). In the context of platform regulation, scholars show that resource asymmetries, primarily around information, between public and platform actors are a potent vehicle for regulatory capture. Laux et al. (2021) argue that platforms influence regulatory audits by purposefully withholding information from unfavourable auditors. Nechushtai (2018) introduces the notion of "infrastructural capture" to describe the fact that actors

tasked with platform oversight are reliant on platform infrastructure, prompting capture. Exploring the impact of information asymmetries between the media, as the fourth estate, and platforms, Dommett (2021) finds that platforms withhold information to obstruct scrutiny. In line with these findings, I argue that resource asymmetries whereby platforms hold a resource advantage over the state prompt risks of regulatory capture in the development of platform regulation in the UK; I refer to this as regulatory capacity capture.

A capacity-based approach to the study of regulation

I argue that the capacity-based approach to the study of regulatory processes pursued in this article advances the research on platform regulation in three central ways. First, by tracing the enrollment of regulatory resources in an emergent regulatory landscape I provide evaluative assessments of actor-specific regulatory capacity. Second, in highlighting resource deficits and asymmetries in state-platform interplay, the capacity-based approach offers decisional insights into the processes and challenges related to regulatory development. Third, by analytically pinpointing capacity-based challenges, the approach enables arguments into the feasibility and recommendations for necessary strategies for overcoming these challenges in regulating online platforms.

Table 1: Regulatory capacity and resources

REGULATORY RESOURCE	DEFINITION
Information	Specialist and technical information that is relevant to policy decisions; information about regulatee behaviour; ability to access timely, relevant and reliable information.
Authority	Possession of legal or de facto power to demand, forbid, guarantee and adjudicate; authority means that what an actor requires makes a practical difference to the way other actors act.
Treasure	Possession of financial resources or fungible money that enables the possession, exchange, or access to other relevant regulatory resources.
Organised expertise	Professionalised staff with expert knowledge and know-how relevant to regulatory processes.

Source: Author's own conceptualisation of regulatory capacity drawing from Black's six-part model of regulatory capacity; Hood's four-part framework of tools of government; and Margetts's work on computerising the tools of government, and the synthesis of interview data collected for this research (Black, 2003; Hood, 1983; Hood & Margetts, 2007; Margetts, 1998).

The United Kingdom as case study in internet policy development

To reveal context-rich descriptions of regulatory processes within a case, interview-based methods are frequently used in platform regulation scholarship, for example to study regulatory contexts in Australia (Duguay et al., 2020), Germany (Gorwa, 2021), the UK (Dommett, 2021; Dommett & Zhu, 2022), and the United States (Kadri & Klonick, 2019; Kettemann & Schulz, 2020). This research employs an interview-based case study of the emergent regulatory landscape in the UK. Building on Dommett and Zhu's (2022) research on the OSB, I adopt an instrumental approach "to provide insight into a particular issue [and] redraw generalisations" (Mills et al., 2010). I seek to create a deep understanding of the emergent regulatory system and reveal transportable patterns for comparison across cases.

The UK was selected as a case study for three reasons. First, the UK is a high-capacity state and leading democracy. Its regulatory trajectory sets precedent for international regulation (Busch et al., 2005). Second, since interest groups historically play a significant role in regulation in the UK (Miller & Dinan, 2008; Wright, 2014) and internet platforms have established an affluent lobby (Lombardi, 2022; Popiel, 2018), this case offers rich context to study state–platform interplay. Third, while the regulation of online safety on internet platforms has been declared a government priority and enjoys the backing of top politicians (Kent et al., 2020), progress on regulation has been repeatedly delayed. Therefore, while the UK case may have unique political aspects, the insights drawn from this research can be relevant and informative for other nations and international bodies that share similar capacity configurations. Examples of such nations and bodies may include those in Europe and the US, where similar concerns have been expressed over the lack of effective platform regulation.

Seeking to create thick descriptions about actor-specific regulatory capacity and how regulatory actors use respective resources towards emergent regulation, I adopt a qualitative, inductive approach using elite interviews. With ethics approval from the University of Oxford, I conducted 33 semi-structured interviews with 34 participants from March 2021 to December 2021 (see table 2 and Appendix A for a list of interviews). During this time period, the OSB was in active development with a new draft bill being introduced in May 2021. All interviews were conducted over Zoom and lasted between 45 and 90 minutes. Interviews were recorded and transcribed. For each interview, I compiled a synthesis memo that selectively identified prominent topics and relevant quotes. Names and organisational affiliations are only mentioned where informed consent was given.

Table 2: Overview of target groups for interviews carried out by the researcher between 26 March 2021 and 16 December 2021

TARGET GROUP	DESCRIPTION	NUMBER OF PARTICIPANTS
Regulator	Staff at regulatory agencies including the Office of Communications (Ofcom), the Competition and Markets Authority (CMA), the Information Commissioner's Office (ICO), the Financial Conduct Authority (FCA), and the Digital Regulation Cooperation Forum (DRCF).	8
Government	Civil servants in government departments and on committees including the Department for Digital, Culture, Media and Sports (DCMS), the DCMS Sub-Committee on Online Harms and Disinformation, and the House of Commons Science and Technology Committee.	11
Industry	Lobbyists and public affairs staff at big tech companies including Google, Meta, Twitter and Snap.	5
CSO and academia	Experts in civil society organisations (CSO) and academia including non-profit organisations, think tanks, fact-checking organisations, universities and legal consultancies.	10

To analyse interview evidence, I make use of inductive open and axial coding moving from descriptive codes to comprehensive themes (Saldana, 2009). This data was supplemented in triangulation with evidence from a document analysis of key policy documents, including transcripts from parliamentary hearings, reports, press releases and other official communications. To identify and select relevant documents for this study, I conducted a comprehensive search of various UK government websites, online databases, and legislative archives. I used a combination of keyword searches for terms related to platform regulation, online harms, and online safety, as well as manual review of search results.

Platform regulation and online safety in the UK, 2000s-2023

In recent years the regulation of platforms has emerged as a pressing issue on the UK's policy agenda in response to concerns over online safety and platform power. But during the 2000s, large internet platforms were celebrated as beacons of democracy, growth, and innovation. They enjoyed what one subject described as a "carte blanche" (interview 23): regulatory freedoms, tax incentives, and safe harbour agreements designed to promote platform investment. Similarly, Poppy Wood, director at Reset and former Downing Street advisor, described how policymakers rolled out a metaphorical "red carpet" (interview 27) to attract big tech business.

However, following what researchers have coined a stream of "public shocks" (Ananny & Gillespie, 2016) – possible foreign interference in the Brexit referendum and the 2016 US elections, the 2017 suicide of teenage girl Molly Russell

that was linked to self-harm content, the 2019 Cambridge Analytica Scandal, the 2020 attacks on 5G infrastructure, and Covid-19 misinformation – there has been sustained and growing regulatory scrutiny of platforms in the UK. As a result, policymakers have examined the government's capacity to regulate platforms under existing legal frameworks (Strowel & Vergote, 2018) and regulatory agencies, including the CMA, ICO, FCA, and Ofcom, have developed codes of conduct and pursued official investigations or litigation.

In 2019, the government of former Prime Minister Theresa May published the Online Harms White Paper that proposed a single regulatory framework to counter a range of online harms. The white paper received mixed reactions, with experts stressing concerns over chilling effects in connection with requirements for content removal (Nash, 2019), but policymakers vowed "to keep momentum" (DCMS & Home Office, 2020). With the start of the Covid-19 pandemic in early 2020, plans to promptly introduce an online safety regime got "caught in the middle of a pandemic and Britain's ongoing divorce from Europe" (Kent et al., 2020, para. 2) and the government announced substantial delays.

At the same time, my interviews reveal that this phase was shaped by heightened state-platform interplay, as the government and platforms collaborated to combat information threats. For example, DCMS, the Department of Health and Social Care (DHSC), and several large platforms including TikTok and YouTube launched a joint public health campaign (DHSC et al., 2021). The government also created the Counter Disinformation Policy Forum, which brought together stakeholders from across government departments, platforms, academia, and civil society to pool resources on content moderation efforts and counter Covid-related misinformation and illegal content (Dinenage & Nichols, 2020).

According to my interviewees, the forum aimed to enhance "consistency and coordination" (interview 2,) and achieve "better information sharing and quicker responses" (interview 7) in times of crisis and mirrored initiatives that had previously been tested for the 2019 general election.

Eventually, in 2021, a revised draft of the OSB was introduced. After several rounds of scrutiny and revision, the OSB was introduced into parliament in 2022 (Walker et al., 2022.). Yet, the bill remained in limbo due to continued delays prompted by ongoing debates over provisions to remove "legal but harmful content" – which were eventually taken out of the bill – and controversial provisions that may require tech companies to weaken end-to-end encryption of content – which were upheld despite vehement criticism from tech firms and privacy and free speech or-

ganisations (Guest, 2023; Hern, 2022, 2023).

Having passed through the two houses of Parliament, in October 2023, the OSB received royal assent and became law as the Online Safety Act (OSA). At its core, the OSA imposes a statutory duty of care platforms towards their users, overseen by Ofcom. The bill requires platforms, depending on their size and functions, to carry out ongoing risk assessments of their services, take measures to mitigate users' exposure to illegal content, and comply with transparency requirements. The scope of the regulation covers user-to-user services, defined as internet services that enable users to generate or share content consumed by other users of the service, as well as certain search engines.

Analysis & findings: capacity capture in an emergent regulatory system for online safety

My interviews reveal wide support for regulatory reform, yet show that, on the ground, policymakers struggle with policy development and nascent regulatory practice. Participants commonly argued that platforms challenge the government's capacity to regulate. Participants described how, as a result, online safety regulation was "stuck" (interview 27) in "regulatory inertia" (interview 20). Paradoxically, this was at the same time that government stakeholders were vigorously preparing for the new regime and were convinced that the OSB would soon give the UK state power over platforms (interview 17). To spotlight regulatory capacity in state-platform interplay and provide decisional insights to explain regulatory development, this research deploys a systematic empirical analysis of four key regulatory resources: information, treasure, authority, and organised expertise. The empirical findings presented here relate exclusively to the development of regulatory policy, though the framework may also prove useful in studying the implementation of regulation. Through an analysis of the relative capacity configurations of the government and platforms, the capacity-based approach is well-equipped to reveal the decisional factors that drive the successes and failures of the UK's emerging regulatory system.

Information

Analysing the state's informational capacity, my interviews reveal there was a wide-reaching "information vacuum" (interview 7) and a "basic lack of information on how platforms act" (interview 13) among regulators vis-à-vis platform regulatees. As a result of information limitations, policy issues related to platforms necessarily remained "ill-defined" (Naik, interview 20) and "opaque" (interview 13),

therefore diminishing government's regulatory capacity. Highlighting the impact of information gaps on emergent regulation, one interviewee argued:

> "We know what is in each pack of cigarettes. And we know every time someone buys it, that that's what they're getting. With tech, with social media, every single person sees something different. And we have no idea why they're seeing what they're seeing and what they're seeing. So that's where the transparency bit comes in, which is: how do we even start to figure out what the harms are and how to regulate it? If right now we don't even know really what the problem is, we can only see that there are bad outcomes". (interview 14)

This statement underscores that policymakers viewed information as a critical, but in this context scarce, resource for policy development. A subject involved in policymaking at a government department put it succinctly: "it's hard to establish [policy] when you don't have the evidence base" (interview 2). Table 3 provides an analytical overview of types of platform data that participants considered relevant to the development of regulation, spanning information about platform practices, policies, and products.

On a bureaucratic level, policymakers struggle to comply with formal requirements for the provision of sufficient evidence in policy processes due to the overall lack of information (interviews 2, 7, 10). Participants described issues around adhering to best practices and government requirements for evidence-based policymaking (see Nutley et al., 2002). For instance, participants described difficulties in sourcing evidence for policy briefings, which then prompted requests for revisions (interviews 9, 19). The effects of this scarcity of information became evident in pre-legislative scrutiny processes for the OSB, which have repeatedly criticised policy proposals on the grounds of insufficient evidence (DCMS & Home Office, 2020; House of Commons DCMS Committee, 2022).

Prompted to discuss the causes of limited informational capacity, participants overwhelmingly attributed them to "information asymmetries … between them [platforms] and any other actors" (interview 13). There was a consensus that platforms hold an information advantage and tightly restrict external access to that information. The interviewees indicated that platforms regularly reject government pleas for information – both broad appeals and concrete requests for particular data, for example around the effects of specific anti-vax policies (interviews 2, 7, 14, 26, 29). Several interviewees argued that platforms purposefully refrain from sharing comprehensive information, in attempts to frustrate government's capacity

to develop regulation (interviews 14, 30). Similarly, an MP argued at an oral evidence hearing that platforms were "kicking all this into the long grass, playing for a bit of time … because it suits [their] purposes" (*Oral Evidence: Online Harms and Disinformation*, 2020, p. 47).

To the extent that platforms share information – for example, through expert hearings, submission of written evidence, multi-stakeholder roundtables, or policy events – interviewees expressed concern about platforms instrumentalising information to yield influence over regulation (interviews 10, 13, 29). Commonly, participants echoed that platforms had established themselves as the sole brokers of information. Thus, civil servants necessarily have to gather information directly from platforms, undermining policymakers' capacity to verify claims and source independent information or supplemental data – potentially putting them at risk of regulatory capture. One interviewee involved in gathering information argued:

> "[When talking to platforms] it was a concern about not being captured or being seen as captured. Platforms have an ability to talk about the specifics in a way that sounds much more authentic and informed than any other actors do. And that's partly because of the information asymmetries that exist". (interview 13)

To that end, participants thought that platforms used bilateral conversations as "an opportunity to say something positive from their perspective" (interview 16) but systematically obscured information about risks and harms (*Oral Evidence: Anti-Vaccination Disinformation*, 2020). For instance, numerous participants maintained that platforms volunteer large amounts of information about harmful but legal content – the subject of ongoing controversy surrounding the OSB – in what Lorna Woods, Professor of Internet Law, who has provided evidence to the government on the OSB, considered a strategic attempt by platforms at "a muddying of the waters by the emphasis on types of content" (Woods, interview 22). Two interviewees reported instances where platform staff shared conflicting information with different policymakers corresponding to the respective policy preferences "like a naughty child between parents" (interview 16; also Orlik, interview 1).

Table 3: Platform data and its accessibility to external parties including government stakeholders

	TYPES OF PLATFORM DATA	SHARING MECHANISM	LEVEL OF GOVERNMENT ACCESS	ACCESS LIMITATIONS
PLATFORM DESIGN AND PRODUCT DEVELOPMENT	Algorithm design, machine learning design, code, developer documentation,	None.	None: no access to platform data.	Trade secrets, NDAs, protected intellectual property, patents,

	TYPES OF PLATFORM DATA	SHARING MECHANISM	LEVEL OF GOVERNMENT ACCESS	ACCESS LIMITATIONS
	A/B testing.			organisational safeguards.
BEHAVIOURAL DATA	Engagement metrics, interaction statistics, A/B testing, aggregate-level and user-level user statistics.	APIs, bespoke data sharing programmes, proprietary analytics tools, proprietary account & ad management tools.	Low: limited access to restricted platform data.	Aggregate-level data only; government often excluded from direct access; government access through third party analysis.
PHENOMENOLOGICAL EVIDENCE	Examples of individual narratives, content moderation decisions and events on platforms.	Bilateral meetings and other interaction, written evidence.	Low: limited access to restricted platform data.	Platform discretion, case by case.
SERVICE AGREEMENTS AND OPERATIONAL DATA	User agreements, terms of service, community guidelines, content moderation guidelines, user policies, aggregate-level content moderation decisions.	Publicly accessible documents, blog posts, announcements, public transparency reports, formal staff presentations.	Medium: public access to restricted platform data.	Publicly available data considered unclear, insufficient or incomplete.

Source: Author's analysis based on interview data collected between 26 March 2021 and 16 December 2021 and document analysis.

Treasure

The analysis reveals major resource asymmetries in treasure, here financial resources available for online safety issues, between the UK government and big platforms. First, looking at the use of treasure as a regulatory resource in platform regulation, the UK government allotted a substantial budget towards platform regulation. Following years of restrictive budgets (HM Treasury, 2020), in 2021 the government allocated "over £110 million … for the passage and implementation of the Online Safety Bill"(HM Treasury, 2021). Many civil servants considered the enhanced budget to be fit for purpose and even generous (interviews 16, 21). However, in comparison to the spending by major platforms, the government budget was marginal. Meta reportedly spent US$13 billion on trust and safety between 2016 and 2021, and Google and Microsoft committed to trust and safety investments of US$30 billion from 2021 to 2026 (Robertson, 2021; Feiner, 2021). Though it is unclear what percentage of this budget was allotted to the UK, this evidence suggests that major platforms hold superior monetary capacity for developing measures to address online safety issues. While participants widely subscribed to the notion of big tech as fiscally affluent, some interviewees raised concerns over resource limitations among smaller companies; interviews 21, 24).

However, it is imperative to note that drawing direct comparisons between government and platform budgets is of limited use, considering the differing scope of measures advanced by public and private actors and costs associated with them. For instance, in the context of illegal and harmful content, government spending may primarily be directed towards oversight, while platforms may focus on investing in human and automated content moderation. Yet as platforms allocate dedicated budgets towards trust and safety measures – potentially addressing certain regulatory concerns – government budgets might be deployed more effectively, strategically addressing the most persistent challenges and providing support to lesser-funded platforms.

However, in the UK context participants raised doubts as to whether platforms used their treasures towards addressing online harms sufficiently. Despite the relative wealth of platforms, participants critiqued tech firms for not contributing adequately to the costs associated with addressing online safety issues. An interviewee at a CSO explained:

> "We have had big industry creating emissions and then regular citizens had to bear a lot of the costs for that. And now we are trying to think of models for how to internalise the costs [of online harms] a little bit more". (interview 14)

This resonates with notions around the internalisation of negative externalities, costs associated with business activities – here, online harms on internet services – that are borne by the public rather than the business (Verveer, 2019). Policymakers widely seek to rebalance asymmetries in treasure through proposals to be implemented in online safety regulation. In this context, interviewees often discussed government-issued fines, but not taxation, as a means to prompt platforms to contribute to offsetting the negative externalities associated with their services. Subjects argued that limits on the existing fines have proven far too low in light of enormous platform treasure (interviews 4, 5).

Across several interviews, participants raised concerns about the potential effects of vast platform treasure. Since policymakers widely view internet services as pillars of innovation and growth, platforms are thought to potentially hold capacity to capture regulatory policymaking by virtue of their enormous value to the UK economy. Interviewees identified tensions between proposals for online safety regulation, on the one hand, and aspirations for “British tech sovereignty” (Naik, interview 20) championed by the government (DCMS, 2021; UK AI Council, 2021) on the other. The issue divided participants. Several subjects described regulation as

a necessary clash between “American tech capital vs. European governments'' (Durham, interview 9) tasked with rebalancing “what’s good for business” with “what’s good for the people'' (interview 10). Others thought that politicians ultimately seek to shield platforms’ interests and business models from overzealous regulatory scrutiny in an effort to sustain their UK ventures. Maria Luisa Stasi, Senior Legal Officer at Article 19, argued:

> "If I were a CEO of a big company, I would say it could have been way worse. Our business model is safe … we just need to be a little more serious on the [voluntary] efforts and tick a few more boxes … We might lose some money, but the entire ship is safe". (Stasi, interview 29)

Finally, my analysis highlighted the use of platform treasure for lobby activities aimed at influencing regulation. Commonly, civil servants considered interactions with platform staff as a type of lobby engagement whereby “platform policy people are basically slightly lobbyists” (interview 11). Across Europe, platforms repeatedly rank among the biggest lobby spenders, with both spending and staff increasing over time (Lombardi, 2022). In the UK, firms regularly sponsor or co-host events alongside government departments, including events focused on platform regulation and issues (for instance, see Westminster eForum, 2022). At the height of political debate on online safety, platforms made substantial donations to political groups (Dickson, 2021) and heavily funded tech-focused civil society and research organisations including fact-checkers and watchdogs (Clarke et al., 2021). Members from these organisations often serve as experts or advisors to the UK government, which raises questions about regulatory capture.

Authority

Against the backdrop of a pending online safety regime, participants considered state authority inadequate for platform regulation. Interviewees emphasised the need for a platform-focused legal mandate which they commonly equated to the yet-to-be-implemented OSB. My interviews showcase how the regulatory agencies, confident in the eventual passage of the bill and the establishment of government’s legal authority over platforms, attempt to mandate platform compliance even while the OSB is still in development and has not been passed; as one subject put it, the agencies “flexed their regulatory muscle” (interview 18). For example, regulatory agencies like the CMA or Ofcom offer voluntary audits for platforms against likely OSB requirements (interview 28). Contrariwise, a handful of participants pointed out lax enforcement of existing authority. They argued that the non-

enforcement of fit-for-purpose legal frameworks on competition, tax and free speech encourages neglectful platform behaviour and results in an underuse of government scrutiny (interviews 20, 27). An interviewee in a high-ranking position at Ofcom argued that as long as the OSB is in development, platforms profit from "a little bit of leeway" (interview 18).

What is more, the interviews indicated that platforms actively challenge existing legal authority. In line with what has been found in other research in this area (Lobel, 2016), participants revealed that platforms habitually exploit legal gaps and political benevolence as an integral strategy of disruptive business models. For example, interviewees accused platforms of profiting from harmful but legal content or dubious advertising practices while being aware of their potential harms. To that extent, platforms regularly pursue litigation against emergent regulatory interventions such as fines or information requests (interview 20).

Beyond firms challenging state authority, the data reveals that platforms, as opposed to the government, are thought of as a source of authority in online safety regulation. Interviewees widely considered platform policies and technology as de facto binding protocols that steer user behaviour, which participants likened to the way in which regulation steers a public. An interviewee from a regulatory agency argued:

> "[Platform] organisations are developing de facto standards by virtue of their market share. That means that everybody has to follow them. And I think we know what we're talking about there, as opposed to potentially what impact a state actor could have on pushing a standard that then is expected to be implemented". (interview 18)

This statement exemplifies that not only do participants acknowledge platform authority over users, but, at least for very large platforms, consider it to be in some ways superior to state authority: due to big tech's enormous user base, measures taken by platforms directly impact users worldwide, whereas state measures only impact users in the UK (interview 5). A member of the DCMS Sub-Committee said: "it's a public policy issue, what [platforms'] internal policies are" (interview 13), treating the public and platform users as the same.

Overwhelmingly, however, interviewees took issue with platform authority. They stressed that their authority lacked legitimacy and due process and noted that platforms fail to use their authority to self-regulate (interviews 2, 5). Even the par-

ticipants who represented platforms expressed unease with the potential impact of their decisions, especially with regard to freedom of speech matters and the representation of minority voices.

Despite those concerns, several instances were discussed in the interviews where the government engaged platform authority to compensate for deficits in government capacity. In this context, interviewees offered various iterations of a similar narrative. Government actors evaluate a situation connected to the spread of harmful but legal content to be an urgent safety threat. Civil servants then share examples of such content with platforms. They demand that platforms deploy their authority in the form of corporate policies. Demands range from general comments on the "suitability" (interview 7) of policies, to demands for content removal or blocking of broad categories of content, to requests from the revision of policies or the creation of new ones altogether (interviews 2, 7, 10). In contrast, interviewees also spoke about trusted flagger programmes, whereby government stakeholders flag individual pieces of content to platforms for priority review against corporate policies. Participants were acutely aware that the government holds no legal authority over harmful content, instead co-opting platform authority to use platform policies and organised expertise to enforce them. An interviewee from a government department recalled complex considerations for engaging platform authority:

> "None of this content is illegal … but we are worried about the effects … we don't want this image spreading, people getting attacked or property damaged, or people get seriously ill and die … but at the same time, we've got to be absolutely sure we're on the right side of democratic principles". (interview 2)

Civil servants demonstrated an intricate knowledge of platform policies. Numerous interviewees explained that policymakers study proprietary platform terms of service agreements (interview 2, 10). . This underscores that while the government co-opts platform authority, they ultimately do so on the platforms' terms. A well-documented example concerned the stern request of Oliver Dowden, then DCMS Secretary of State, for platforms to limit the spread of legal misinformation that linked 5G infrastructure to the spread of coronavirus. After several 5G masts were set on fire in 2020, Dowden reportedly "summoned" (Kelion, 2020) platform staff and demanded stricter policies which platforms reportedly instituted (interviews 3, 24).

Organised expertise

Several interviews pinpointed insufficient technical expertise among public sector staff at government departments and regulatory agencies, causing capacity deficits in platform regulation (interviews 16, 23, 24). According to the assessment of participants, state expertise is often inferior to that of the firms, especially with regard to platform technologies and algorithms. The most severe deficiencies in expertise are attributed to politicians. In particular, high-profile officials are often described as "uniformed" (interview 17) and thought to rely on "lived experience" (interview 16) as private users of internet platforms, resulting in oversimplified notions of complex policy issues (interviews 17, 21, 24). An interviewee working in public affairs for a platform said:

> "I think the bigger risk isn't that people don't understand it. It's the people who think they do understand it … I don't believe many people who regulate the aerospace industry, do you really think they know how planes fly?" (interview 17)

Paradoxically, despite the recognition of deficits, interviewees considered state capacity to be sufficient for the development of novel platform regulation. Participants frequently pointed to similar regulation – the experience of DCMS in broadband spectrum policies, or Ofcom's background in content regulation (interview 21) – as proof of expertise yet failed to mention considerations around the transferability of expertise to platform contexts.

Despite ambiguous views on government expertise, interviews highlighted several government initiatives aimed at building capacity for the emergent platform regulation regime. Participants described a "surge in staffing" (interview 31) at key regulatory offices. Ofcom created 350 new roles for the OSB (Ofcom, 2022) and the CMA launched a unit for overseeing "the most powerful digital firms" (CMA, 2021). Additionally, interviewees described a push towards "greater cooperation on online regulatory matters" (CMA et al., 2021), culminating in the launch of the Digital Regulation Cooperation Forum (DRCF), which is tasked with pooling organised expertise across key agencies regulating the digital sphere.

Other than building up in-house capacity, the government relies on input from platforms to supplement insufficient organised expertise. As detailed in the section on authority, the government hosts regular meetings with major platforms, especially in times of crisis. These meetings aim at establishing a "collective under-

standing" of the information environment though not "a collective response", according to a participant from a government department (interview 7). But according to several interviewees, there are "grey area conversations" (interview 7) in which the government called on platforms to deploy, not only their authority, but organised expertise to counter emerging threats. My analysis documented several instances where officials asked platform personnel to moderate content by deploying organised expertise in the form of human or technical content moderation. Civil servants widely acknowledged that the government does not have sufficient staff or technical resources to moderate content at scale, but generally thought that large platforms hold adequate organised expertise (interview 2, 7). Interviewees voiced concerns about the appropriate level of government involvement without a legal mandate yet stressed the need for agile interventions at scale – and according to participants, this cannot be accommodated through lengthy lawmaking processes such as the OSB, thus necessitating platforms' organised expertise (interviews 2, 7, 16, 17).

Conversely, my interviews at the same time revealed rivalry over organised expertise. The public and private sectors were in direct competition for highly skilled, technical talent. To level up with platform salaries, the government has overhauled salary structures for technical roles. A participant from a regulatory agency explained:

> "There was a limited talent pool available anyway in the country. Because you had to have taken an altruistic approach to end up working in [the public sector] …. Now we can actually get employed on a proper salary, which is always nice, and the skill sets we have range across all the different spectrums, networks, cybersecurity, image text classification". (interview 18)

Highlighting the interplay of states and platforms around organised expertise, my analysis reveals evidence of a revolving-door problem, whereby high-level government employees move to public affairs roles at platforms. Among my interview subjects, of the five subjects working in industry four previously held roles in UK government departments, including at DCMS and the Cabinet Office. One the other hand, none of the subjects working in government were previously affiliated with industry. What is more, experts have pointed out patterns of platforms hiring high-ranking staff at UK government departments and regulatory agencies as well as politicians in policy roles (Courea, 2022; Gemmell, 2021). Perhaps most prominently, Nick Clegg, a former Deputy Prime Minister has been the head of global affairs at Meta since 2022. According to Corporate Europe Observatory around three quar-

ters of Google and Meta's lobbyists that hold or held European Parliament accreditation in 2022 have formerly worked at a governmental body (LobbyControl, 2022). Researchers have connected revolving-door problems with regulatory capture and spill-over effects of sensitive organisational expertise (Dal Bó, 2006).

Interim conclusion

Summarising the central findings of my analysis, I argue that, firstly, the government lacks information on platform activities, and so relies on platforms to provide this resource; but platforms purposefully restrict information in order to challenge regulation. Second, both states and platforms possess substantial, though disparate, treasure for online safety regulation, however regulation may be necessary to direct platform resources towards offsetting the societal costs of their service. Third, there is a gap in organised expertise, though the government increasingly competes with platforms for limited resources and informally requests that platforms deploy their organised expertise at scale. Fourth, against the backdrop of an emergent regime, and therefore enhanced government legal authority, platforms hold de facto authority over their users, and the government engages corporate authority towards content moderation without a formal mandate.

Discussion

In this chapter, I have proposed and implemented a capacity-based approach to the study of the emerging system for platform regulation in the UK. Distilling and expanding on traditional models of governance and regulation (Black, 2003; Hood, 1983; Hood & Margetts, 2007), I have identified four salient capacities that are central to the regulation of digital technologies. I deploy the capacity-based approach to trace relative resource configurations of public and private actors in interplay, revealing persistent capacity deficits and asymmetries. Finally, in this section I discuss the feasibility of strategies for overcoming the capacity challenges identified.

My empirical work has showcased that state capacity is interwoven with platform resources in complex ways that prompt resource interdependencies and rivalry but that also hold potential for collaboration. Therefore, I have argued that regulatory capacity is relative and best understood as a function of its resource position in relation to platforms. Examining state-platform interplay, I have revealed capacity asymmetries prompting risks of regulatory capture whereby platforms use their resources to influence and impede regulatory development. Thus, this analysis offers not only evaluative assessments of resource configurations but also explanatory

insights that illuminate regulatory development.

To bring these findings into dialogue with the emergent regulatory regime, in what follows I discuss regulatory capacities in the context of the OSA (Online Safety Act, 2023). While the implementation of the act is ongoing at the time of publication, my aim is to discuss whether the overarching regulatory approach outlined in the act is equipped to mitigate capacity-based challenges to regulation.

Risk assessments, safety duties, and terms of service

The OSA mandates that platforms conduct risk assessments on their services, including design, operation, and content, to evaluate the risk of users encountering illegal content (Part 3, Chapter 2, Section 9). For services likely to be accessed by children, a separate risk assessment is required to evaluate the harm to children from harmful content (Part 3, Chapter 2, Section 11). The Act also imposes safety duties on platforms, requiring them to adopt proportionate measures to mitigate risks through content moderation, technical features, and user support measures (Part 3, Chapter 2, Section 10). Additionally, the OSA creates a duty for platforms to adopt clear and accessible terms of service and consistently apply them to protect users from illegal or harmful content, such as setting out terms to prevent children of a certain age from accessing a service (Part 3, Chapter 2, Sections 10 & 12). The OSA leverages the platforms' organised expertise – in this context, predominantly staff and technology – to identify and mitigate risks associated with complex technologies, system-level outcomes, and content enabling the government to utilise superior platform capacity while also pre-empting issues related to limited government resources given the scale of services and content in scope. In line with findings from the interviews, in the implementation of the OSA the government recognises the *authority* of platform rules in steering users. The act actively enlists platform authority in its implementation of an online safety regime, requiring platforms to define and apply proprietary rules for the mitigation of illegal and harmful content.

Information powers and transparency requirements

Secondly, the OSA grants Ofcom wide-reaching information powers to request from platforms "any information that they [Ofcom] require for the purpose of exercising, or deciding whether to exercise, any of their only safety functions" (Part 7, Chapter 4, Section 100). This includes information necessary to assess compliance, evaluate technology accuracy and effectiveness, and carry out research on online safety issues, such as illegal content and user exposure to risks (Part 7, Chapter 4,

Section 100). Under these provisions, Ofcom will also be authorised to view information demonstrating the operation of systems, including algorithms, in real time (Part 7, Chapter 4, Section 100). However, all information must be proportionate to the use to which the information is to be put in the exercise of regulatory functions. Ofcom also has the authority to appoint skilled persons within a company to provide reports for compliance assessments and risk understanding (Part 7, Chapter 4, Section 104). The OSA requires platforms to produce regular transparency reports (Part 4, Chapter 5, Section 77). These provisions directly relate to platforms' regulatory capacities. With these substantial information powers, Ofcom can help address persistent information asymmetries, which will enhance the government's resource position in *information*. Going forward, the government's increased information capacity can inform a more data-driven decision-making on the use and development of other capacities. Additionally, the government enrols platforms' *organised expertise* by requiring firms to collect and make information on online safety issues accessible in reports (Part 4, Chapter 5, Section 77).

Enforcement powers, codes of practice, and guidance

Finally, the OSA empowers Ofcom to oversee and enforce compliance with the new regulations and corresponding duties, including the ability to issue penalties of up to 10% of a platform's annual global revenue or daily rate penalties for ongoing non-compliance (Part 7, Chapter 6, Section 137 & Schedule 13). Thus, the OSA allows for the distribution to the government of substantial *treasure* from platforms that violate the law. Ofcom may also seek court orders to impose business disruption measures in the most serious cases, which could revoke a platform's access to third-party services such as internet service providers or payment services (Part 7, Chapter 6, Section 144-148). Additionally, Ofcom will be required to produce codes of practice that specify the measures that platforms must take to comply with the various requirements and provide guidance documents on how platforms can institute this (Part 3, Chapter 6). However, experts argue that adherence to the codes of practice may not be mandatory but would establish a presumption of compliance with the relevant duty (Heywood, 2022). To summarise, the OSA invests considerable *authority* in Ofcom and creates a legal basis for government intervention in online safety related platform matters, while placing a significant burden on Ofcom to help companies understand evolving risks and compliance requirements. Yet while the risk-based approach enlists some platform authority, ultimate authority lies with Ofcom and UK courts.

When examining the OSA with regards to regulatory capacity, it becomes evident that platform regulation in the UK will remain characterised by a complex inter-

play between the state and platforms, even after the implementation of the Act. The approach relies on a risk-based duty of care, and this enrols private firms in regulation and requires platforms to use their proprietary capacities, including authority and organised expertise, to develop and enforce measures that comply with the regulatory framework. This allows the government to tap into the superior resources of platforms while avoiding substantial investments in internal capacity building. What is more, under the OSA, the government can also acquire resources held by platforms – primarily information – to level the capacity asymmetry between them.

Despite this increased access to regulatory resources, the relative scarcity of resources in government, in contrast to the resource richness of large platforms, persists. This asymmetric resource constellation not only diminishes the government's capacity to act as a regulator, but it also elevates platforms to a position where they can use resources to capture regulatory processes by strategically withholding or leveraging resources for gain.

Yet this is where perhaps the OSA's most significant achievement comes into play. In creating a legal basis to regulate what some have considered a lawless "Wild West" and in empowering Ofcom to oversee and enforce platform's compliance with the regime, the Act enables the UK government to establish authority over private platforms. Nevertheless, the risk-based approach still leaves the platforms with substantial leeway, particularly as codes of practice and guidance will only become established upon the initial implementation of the Act. If the government remains short on essential regulatory capacities in the future and entirely reliant on the platforms to access relevant resources, the successful implementation of the OSA rests primarily on the government's legal authority and its ability to devise and enforce policies for good governance.

Further research is needed to determine if the framework of regulatory capacity and its four salient resources can explain regulatory processes across other governments and regulatory sectors related to digital technology. It is also necessary to study how platforms' capacity can be enrolled in formal regulation while mitigating the risks of capture. While this study narrowly focuses on state-platform interplay, civil society organisations and research institutions are likely loci of regulatory capacity that remain unexplored here. A systematic analysis of government, state, and civic actors with regard to their capacity to fulfil regulatory functions could offer an important empirical perspective to inform the ideal enrolment of actors and their respective resources in regulation going forward.

Conclusion

In this article, I have examined the UK's emergent online safety regime as a case study to investigate why even high-capacity, well-resourced democracies grapple with the regulation of internet platforms. Drawing from regulatory theory, I have proposed an original framework of four salient resources for the analysis of regulatory capacity in technology regulation. I have presented an original data set of 33 elite interviews with subjects from government, regulatory agencies, digital platforms, and civil society, in triangulation with a document analysis of government communications. The study makes a number of important findings. First, the government lacks key regulatory resources, resulting in a persistent capacity deficit. Second, there are persistent resource asymmetries between states and platforms, with platforms holding a capacity advantage. Third, the asymmetric resource constellation leads to a risk of regulatory capture, whereby platforms exploit government's reliance on their resources. Finally, applying these findings to the Online Safety Act, I have argued that the Act contains provisions that capacitate the government to enrol platform resources in ways that preempt regulatory capture, by setting rules that require platforms to share and make their resources accessible and by specifying how they should do so. However, the success of this approach depends on the government's ability to effectively oversee and enforce the regulatory regime.

References

Ananny, M., & Gillespie, T. (2016). *Public platforms: Beyond the cycle of shocks and exceptions*. 22. https://blogs.oii.ox.ac.uk/ipp-conference/2016/programme-2016/track-b-governance/platform-studies/tarleton-gillespie-mike-ananny.html

Au, C. H., Ho, K. K. W., & Chiu, D. K. W. (2021). The role of online misinformation and fake news in ideological polarization: Barriers, catalysts, and implications. *Information Systems Frontiers*, *24*, 1331–1354. https://doi.org/10.1007/s10796-021-10133-9

Barnes, T. (2022, September 13). *The Online Safety Bill will be taken forward*. Simons Muirhead Burton. https://www.smb.london/news/the-online-safety-bill-will-be-taken-forward/

Barrett, B., Dommett, K., & Kreiss, D. (2021). The capricious relationship between technology and democracy: Analyzing public policy discussions in the UK and US. *Policy & Internet*, *13*(4), 522–543. https://doi.org/10.1002/poi3.266

Black, J. (2002). Mapping the contours of contemporary financial services regulation. *Journal of Corporate Law Studies*, *2*(2), 253–287. https://doi.org/10.1080/14735970.2002.11419886

Black, J. (2003). Enrolling actors in regulatory systems: Examples from UK financial services regulation. *Public Law*, 63–91.

Bradshaw, S., Neudert, L.-M., & Howard, P. N. (2018). *Government responses to malicious use of social media* [Report]. NATO Strategic Communications Centre of Excellence. https://www.stratcomcoe.org/government-responses-malicious-use-social-media

Busch, P.-O., Jörgens, H., & Tews, K. (2005). The global diffusion of regulatory instruments: The making of a new international environmental regime. *The ANNALS of the American Academy of Political and Social Science*, *598*(1), 146–167. https://doi.org/10.1177/0002716204272355

Chadwick, A. (2013). *The hybrid media system: Politics and power* (1st ed.). Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199759477.001.0001

Chan, N. K., & Kwok, C. (2021). Guerilla capitalism and the platform economy: Governing Uber in China, Taiwan, and Hong Kong. *Information, Communication & Society*, *24*(6), 780–796. https://doi.org/10.1080/1369118X.2021.1909096

Clarke, L., Williams, O., & Swindells, K. (2021, July 30). How Google quietly funds Europe's leading tech policy institutes. *New Statesman*. https://www.newstatesman.com/science-tech/big-tech/2021/07/how-google-quietly-funds-europe-s-leading-tech-policy-institutes

Coe, P. (2022). The draft Online Safety Bill and the regulation of hate speech: Have we opened Pandora's box? *Journal of Media Law*, *14*(1), 50–75. https://doi.org/10.1080/17577632.2022.2083870

Competition and Markets Authority. (2021). *Digital markets unit* [Collection]. UK Government. https://www.gov.uk/government/collections/digital-markets-unit

Competition and Markets Authority, Information Commissioner's Office, Ofcom, & Financial Conduct Authority. (2021). *The digital regulation cooperation forum* [Collection]. UK Government. https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum

Courea, E. (2022, March 2). Facebook ramps up UK lobbying hires as privacy battles loom. *Politico*. https://www.politico.eu/article/meta-facebook-ramps-up-uk-eu-lobbying-hires-privacy-battles/

Dal Bó, E. (2006). Regulatory capture: A review. *Oxford Review of Economic Policy*, *22*(2), 203–225. https://doi.org/10.1093/oxrep/grj013

DeNardis, L., & Hackl, A. M. (2015). Internet governance by social media platforms. *Telecommunications Policy*, *39*(9), 761–770. https://doi.org/10.1016/j.telpol.2015.04.003

Department for Digital, Culture, Media & Sport. (2021). *The UK safety tech sector: 2021 analysis* [Independent report]. UK Government. https://web.archive.org/web/20220601013924/https://www.gov.uk/government/publications/safer-technology-safer-users-the-uk-as-a-world-leader-in-safety-tech/the-uk-safety-tech-sector-2021-analysis

Online Safety Bill, HL Bill 87, UK Parliament (2022). https://bills.parliament.uk/publications/49376/documents/2822

Department for Digital, Culture, Media & Sport. (2022a). *Digital regulation: Driving growth and unlocking innovation* [Policy paper]. UK Government. https://web.archive.org/web/20221221175641/https://www.gov.uk/government/publications/digital-regulation-driving-growth-and-unlocking-innovation/digital-regulation-driving-growth-and-unlocking-innovation

Department for Digital, Culture, Media & Sport. (2022b). *Fact sheet on changes to the illegal content duties within the Online Safety Bill* [Guidance]. UK Government. https://web.archive.org/web/20221006023927/https://www.gov.uk/government/publications/fact-sheet-on-changes-to-the-illegal-content-duties-within-the-online-safety-bill/fact-sheet-on-changes-to-the-illegal-content-duties-withi

n-the-online-safety-bill

Department for Digital, Culture, Media & Sport & Home Office. (2020). *Online harms white paper: Full government response to the consultation* (White Paper 354). HMSO. https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response

Department of Health and Social Care, Zahawi, N., Dowden, O., & Hancock, M. (2021). *Leading social media platforms unite to support COVID-19 vaccine drive* [Press release]. UK Government. https://www.gov.uk/government/news/leading-social-media-platforms-unite-to-support-covid-19-vaccine-drive

Dickson, A. (2021, April 22). UK lobbying questions raised by big tech cash for MP interest groups. *Politico*. https://www.politico.eu/article/uk-lobbying-big-tech-cash-mp-interest-groups/

Dinenage, C., & Nichols, C. (2020). *Internet: Disinformation. Question for Department for Digital, Culture, Media and Sport* (Written questions, answers and statements UIN 124329). UK Parliament. https://questions-statements.parliament.uk/written-questions/detail/2020-12-02/124329

Dittel, A. (2022). The UK's Online Safety Bill: The day we took a stand against serious online harms or the day we lost our freedoms to platforms and the state? *Journal of Data Protection & Privacy*, *5*(2), 183–194.

Dommett, K. (2021). The inter-institutional impact of digital platform companies on democracy: A case study of the UK media's digital campaigning coverage. *New Media & Society*, *25*(10), 2763–2780. https://doi.org/10.1177/14614448211028546

Dommett, K., & Zhu, J. (2022). The barriers to regulating the online world: Insights from UK debates on online political advertising. *Policy & Internet*, *14*(4), 772–787. https://doi.org/10.1002/poi3.299

Duguay, S., Burgess, J., & Suzor, N. (2020). Queer women's experiences of patchwork platform governance on Tinder, Instagram, and Vine. *Convergence: The International Journal of Research into New Media Technologies*, *26*(2), 237–252. https://doi.org/10.1177/1354856518781530

Farrell, H., & Newman, A. L. (2010). Making global markets: Historical institutionalism in international political economy. *Review of International Political Economy*, *17*(4), 609–638. https://doi.org/10.1080/09692291003723672

Flew, T., & Gillett, R. (2021). Platform policy: Evaluating different responses to the challenges of platform power. *Journal of Digital Media & Policy*, *12*(2), 231–246. https://doi.org/10.1386/jdmp_00061_1

Flew, T., Gillett, R., Martin, F., & Sunman, L. (2021). Return of the regulatory state: A stakeholder analysis of Australia's Digital Platforms Inquiry and online news policy. *The Information Society*, *37*(2), 128–145. https://doi.org/10.1080/01972243.2020.1870597

Gemmell, K. (2021, December 20). Facebook hires top lawyer from U.K.'s antitrust watchdog. *Bloomberg*. https://www.bloomberg.com/news/articles/2021-12-20/revolving-doors-in-metaverse-as-facebook-hires-watchdog-s-lawyer

Gillespie, T. (2018). Regulation of and by platforms. In J. Burgess, A. Marwick, & T. Poell (Eds.), *The Sage handbook of social media* (pp. 254–278). SAGE Publications Ltd. https://doi.org/10.4135/9781473984066

Gorwa, R. (2019). What is platform governance? *Information, Communication & Society*, *22*(6), 854–871. https://doi.org/10.1080/1369118X.2019.1573914

Gorwa, R. (2021). Elections, institutions, and the regulatory politics of platform governance: The case of the German NetzDG. *Telecommunications Policy*, *45*(6). https://doi.org/10.1016/j.telpol.2021.102145

Gorwa, R., Binns, R., & Katzenbach, C. (2020). Algorithmic content moderation: Technical and political challenges in the automation of platform governance. *Big Data & Society*, *7*(1). https://doi.org/10.1177/2053951719897945

Guest, P. (2023, October 26). The UK's controversial online safety act is now law. *Wired*. https://www.wired.com/story/the-uks-controversial-online-safety-act-is-now-law/

Helm, T. (2022, November 13). UK government criticised for failing to protect children from online harm. *The Observer*. https://www.theguardian.com/technology/2022/nov/13/uk-government-criticised-for-failing-to-protect-children-from-online-harm

Hern, A. (2022, November 29). Changes to Online Safety Bill tread line between safety and appearing 'woke'. *The Guardian*. https://www.theguardian.com/technology/2022/nov/29/changes-to-online-safety-bill-tread-line-between-safety-and-appearing-woke

Hern, A. (2023, April 18). WhatsApp and Signal unite against Online Safety Bill amid privacy concerns. *The Guardian*. https://www.theguardian.com/technology/2023/apr/18/whatsapp-signal-unite-against-online-safety-bill-privacy-messaging-apps-safety-security-uk

HM Treasury. (2020). *Spending review 2020* [Policy paper]. UK Government. https://www.gov.uk/government/publications/spending-review-2020-documents/spending-review-2020

HM Treasury. (2021). *Autumn budget and spending review 2021. A stronger economy for the British people* (Report HC 822). House of Commons. https://assets.publishing.service.gov.uk/media/61c49602e90e07196a66be73/Budget_AB2021_Web_Accessible.pdf

Hoffmann-Riem, W. (2020). Artificial intelligence as a challenge for law and regulation. In T. Wischmeyer & T. Rademacher (Eds.), *Regulating artificial intelligence* (pp. 1–29). Springer International Publishing. https://doi.org/10.1007/978-3-030-32361-5_1

Hood, C. C. (1983). *Tools of government* (1st ed.). Red Globe Press. https://doi.org/10.1007/978-1-349-17169-9

Hood, C., & Margetts, H. (2007). *The tools of government in the digital age* (2nd ed.). Palgrave Macmillan.

House of Commons & Digital, Culture, Media and Sport Committee. (2022). *The Draft Online Safety Bill and the legal but harmful debate: Government response to the Committee's eighth report* (Special Report HC 1221; pp. 1–36). House of Commons. https://committees.parliament.uk/publications/9407/documents/161164/default/

Howard, P. N. (2020). *Lie machines: How to save democracy from troll armies, deceitful robots, junk news operations, and political operatives*. Yale University Press. https://doi.org/10.2307/j.ctv10sm8wg

Howard, P. N., & Hussain, M. M. (2013). *Democracy's fourth wave? Digital media and the arab spring*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199936953.001.0001

Instrumental case study. (2010). In *Encyclopedia of case study research* (pp. 474–475). SAGE Publications, Inc. https://doi.org/10.4135/9781412957397.n175

Kadri, T. E., & Klonick, K. (2019). Facebook v. Sullivan: Public figures and newsworthiness in online speech. *Southern California Law Review*, *93*, 1–37. https://doi.org/10.2139/ssrn.3332530

Kelion, L. (2020, April 5). Coronavirus: Tech firms summoned over 'crackpot' 5G conspiracies. *BBC News*. https://www.bbc.com/news/technology-52172570

Kent, J., Kirkham, J., Ward, C., & The Children's Media Foundation Executive Committee. (2020, December 2). Whatever happened to the online harms bill? [Blog post]. *Media@LSE*. https://blogs.lse.ac.uk/medialse/2020/12/02/whatever-happened-to-the-online-harms-bill/

Kettemann, M. C., & Schulz, W. (2020). *Setting rules for 2.7 billion: A (first) look into Facebook's norm-making system: Results of a pilot study* (Working Paper 1; Working Papers of the Hans-Bredow-Institut, pp. 1–34). Leibniz Institute for Media Research. https://doi.org/10.21241/ssoar.71724

Klonick, K. (2017). The new governors: The people, rules, and processes governing online speech. *Harvard Law Review*, *131*(6), 1598–1670.

Laux, J., Wachter, S., & Mittelstadt, B. (2021). Taming the few: Platform regulation, independent audits, and the risks of capture created by the DMA and DSA. *Computer Law & Security Review*, *43*. https://doi.org/10.1016/j.clsr.2021.105613

Levi-Faur, D. (2011). Regulation and regulatory governance. In D. Levi-Faur (Ed.), *Handbook on the politics of regulation* (pp. 3–24). Edward Elgar Publishing. https://doi.org/10.4337/9780857936110.00010

LobbyControl. (2022, September 20). *The revolving door – from public officials to big tech lobbyists*. Corporate Europe Observatory. https://corporateeurope.org/en/2022/09/revolving-door-public-officials-big-tech-lobbyists

Lobel, O. (2016). The law of the platform. *Minnesota Law Review*, *101*, 87–166.

Lombardi, P. (2022, March 22). Big tech boosts lobbying spending in Brussels. *Politico*. https://www.politico.eu/article/big-tech-boosts-lobbying-spending-in-brussels/

Margetts, H. (1998). Computerising the tools of government? In I. Th. M. Snellen & W. B. H. J. van de Donk (Eds.), *Public administration in an information age: A handbook* (pp. 441–460). IOS Press. https://ebooks.iospress.nl/volume/public-administration-in-an-information-age

Margetts, H., John, P., Hale, S., & Yasseri, T. (2016). *Political turbulence: How social media shape collective action*. Princeton University Press. https://doi.org/10.2307/j.ctvc773c7

Mason, R. (2017, November 14). Theresa May accuses Russia of interfering in elections and fake news. *The Guardian*. https://www.theguardian.com/politics/2017/nov/13/theresa-may-accuses-russia-of-interfering-in-elections-and-fake-news

Miller, D., & Dinan, W. (2008). Corridors of power: Lobbying in the UK. *Observatoire de La Société Britannique*, *6*, 25–45. https://doi.org/10.4000/osb.409

Nash, V. (2019). Revise and resubmit? Reviewing the 2019 Online Harms White Paper. *Journal of Media Law*, *11*(1), 18–27. https://doi.org/10.1080/17577632.2019.1666475

Nechushtai, E. (2018). Could digital platforms capture the media through infrastructure? *Journalism*, *19*(8), 1043–1058. https://doi.org/10.1177/1464884917725163

Neudert, L.-M. (2020). Hurdles and pathways to regulatory innovation in digital political campaigning. *The Political Quarterly*, *91*(4), 713–721. https://doi.org/10.1111/1467-923X.12915

Nutley, S., Davies, H., & Walter, I. (2002). *Evidence based policy and practice: Cross sector lessons from the UK* (Working Paper 9). ESRC UK Centre for Evidence Based Policy and Practice. https://www.rese

archgate.net/publication/251786301_Evidence_Based_Policy_and_Practice_Cross_Sector_Lessons_From_the_UK

Ofcom. (2022). *Online Safety Bill: Ofcom's roadmap to regulation* [Roadmap]. https://www.ofcom.org.uk/__data/assets/pdf_file/0016/240442/online-safety-roadmap.pdf

Online Safety Act 2023, (2023). https://www.legislation.gov.uk/ukpga/2023/50/enacted

Oral evidence: Anti-vaccination disinformation (Evidence HC 1049; pp. 1–47). (2020). House of Commons. https://committees.parliament.uk/oralevidence/1446/pdf/

Oral evidence: Online harms and disinformation (Evidence HC 234). (2020). House of Commons. https://committees.parliament.uk/oralevidence/458/pdf/

Papaevangelou, C. (2021). The existential stakes of platform governance and online content regulation: A critical conceptual model [version 2; peer review: 3 approved]. *Open Research Europe*, *1*, 31. https://doi.org/10.12688/openreseurope.13358.1

Popiel, P. (2018). The tech loobby: Tracing the contours of new media elite lobbying power. *Communication, Culture and Critique*, *11*(4), 566–585. https://doi.org/10.1093/ccc/tcy027

Robertson, A. (2021, September 21). Facebook says it's spent $13 billion on 'safety and security' since 2016. *The Verge*. https://www.theverge.com/2021/9/21/22685863/facebook-safety-security-staff-spending-misinformation-abuse-wall-street-journal-reports

Saldana, J. (2009). *The coding manual for qualitative researchers* (1st ed.). SAGE Publications.

Schlesinger, P. (2022). The neo-regulation of internet platforms in the United Kingdom. *Policy & Internet*, *14*(1), 47–62. https://doi.org/10.1002/poi3.288

Scott, M., & Dickson, A. (2023, February 28). How UK's Online Safety Bill fell victim to never-ending political crisis. *Politico*. https://www.politico.eu/article/online-safety-bill-uk-westminster-politics/

Strowel, A., & Vergote, W. (2018). *Digital platforms: To regulate or not to regulate? Message to regulators: Fix the economics first, then focus on the right regulation* (pp. 1–16) [Report]. European Commission. https://ec.europa.eu/information_society/newsroom/image/document/2016-7/uclouvain_et_universit_saint_louis_14044.pdf

Suzor, N. P. (2019). *Lawless: The secret rules that govern our digital lives*. Cambridge University Press. https://doi.org/10.1017/9781108666428

Taeihagh, A., Ramesh, M., & Howlett, M. (2021). Assessing the regulatory challenges of emerging disruptive technologies. *Regulation & Governance*, *15*(4), 1009–1019. https://doi.org/10.1111/rego.12392

The Conservative and Unionist Party. (2017). *Forward, together. Our plan for a stronger Britain and a prosperous future* [Election manifesto]. https://general-election-2010.co.uk/2017-general-election-manifestos/conservative-manifesto-2017.pdf

Theil, S. (2019). The Online Harms White Paper: Comparing the UK and German approaches to regulation. *Journal of Media Law*, *11*(1), 41–51. https://doi.org/10.1080/17577632.2019.1666476

Trengove, M., Kazim, E., Almeida, D., Hilliard, A., Zannone, S., & Lomas, E. (2022). A critical review of the Online Safety Bill. *Patterns*, *3*(8). https://doi.org/10.1016/j.patter.2022.100544

UK AI Council. (2021). *AI roadmap* (pp. 1–37) [Independent report]. House of Lords Select Committee on Democracy and Digital Technologies. https://www.gov.uk/government/publications/a

i-roadmap

Verveer, P. (2019). *Countering negative externalities in digital platforms* [Policy paper]. Shorenstein Center on Media, Politics and Public Policy. https://shorensteincenter.org/countering-negative-externalities-in-digital-platforms/

Walker, A., Ratcliffe, E., & Certo, M. (2022, March 17). *Online Safety Bill introduced in Parliament* [News]. TechUK. https://www.techuk.org/resource/online-safety-bill-introduced-in-parliament.html

Westminster eForum. (2022). *The draft Online Safety Bill and next steps for online regulation in the UK* [Conference website for UK-wide public policy events]. https://www.westminsterforumprojects.co.uk/publication/online-reg-22

Wood, P. (2021, September 29). *Interview 27* [Personal communication].

Woods, L. (2019). The duty of care in the Online Harms White Paper. *Journal of Media Law*, *11*(1), 6–17. https://doi.org/10.1080/17577632.2019.1668605

Wright, J. (2014). Regional variation in Chinese internet filtering. *Information, Communication & Society*, *17*(1), 121–141. https://doi.org/10.1080/1369118X.2013.853818

Wylie, C. (2019). *Mindf*ck: Inside Cambridge Analytica's plot to break the world* (Export/Airside). Profile Books.

Yadav, K., Erdoğdu, U., Siwakoti, S., Shapiro, J. N., & Wanless, A. (2021). Countries have more than 100 laws on the books to combat misinformation. How well do they work? *Bulletin of the Atomic Scientists*, *77*(3), 124–128. https://doi.org/10.1080/00963402.2021.1912111

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Profile Books.

Appendix A

Table 1: List of interviews carried out by the researcher between 26 March 2021 and 16 December 2021 (including those where participants requested anonymity)

ID	NAME	TYPE	ORGANISATION	TITLE	PREVIOUS OR CURRENT APPOINTMENTS IF RELEVANT	DATE
1	Edward Orlik	Government	Cabinet Office Internet Policy Team	Senior Policy Advisor		26 Mar 21
2		Government				06 Mar 21
3	Nicola Aitken	CSO/ academia	Full Fact	Policy and Government Relations Manager		07 Apr 21
4	Emily Taylor	CSO/ academia	Oxford Information Labs	CEO		07 Apr 21
5	Chloe Colliver	CSO/ academia	Institute for Strategic Dialogue	Head of Digital Policy & Strategy	Current: Head of Industry Developments at Ofcom	12 Apr 21

ID	NAME	TYPE	ORGANISATION	TITLE	PREVIOUS OR CURRENT APPOINTMENTS IF RELEVANT	DATE
6	Phoebe Arnold	CSO/ academia	Full Fact	Partnerships Manager		16 Apr 21
7		Government				21 Apr 21
8	Christian Schwieter	CSO/ academia	Institute for Strategic Dialogue	Policy & Research Analyst		26 Apr 21
9	Conor Durham	Government	DCMS Sub-Committee on Online Harms and Disinformation	Digital and Technology Specialist		27 Apr 21
10		Government				02 Jun 21
11		Government				06 Jun 21
12	Pierre Andrews	Government	UK Parliament	Senior Parliamentary Assistant to Damien Collins		18 Jun 21
13		Government				15 Jul 21
14		CSO/ academia				16 Jul 21
15	[two interviewees]	Industry			Previous: Government	16 Aug 21
16		Government				26 Aug 21
17		Industry			Previous: Government	27 Aug 21
18		Regulator				27 Aug 21
19		Government				02 Sept 21
20	Ravi Naik	CSO/ academia	AWO; Oxford Internet Institute	Legal Director; Visiting Fellow		08 Sept 21
21		Regulator				13 Sept 21

ID	NAME	TYPE	ORGANISATION	TITLE	PREVIOUS OR CURRENT APPOINTMENTS IF RELEVANT	DATE
22	Lorna Woods	CSO/ academia	University of Essex	Professor of Internet Law		15 Sept 21
23		Industry			Previous: Government	16 Sept 21
24		Industry			Previous: Government	17 Sept 21
25		Regulator				17 Sept 21
26		Regulator				28 Sept 21
27	Poppy Wood	CSO/ academia	Reset	Senior Advisor	Previous: Advisor to Prime Minister's Office (2012-14)	29 Sept 21
28	Simon McDougall	Regulator	ICO (previous employer)	Former Deputy Commissioner, Executive Director	Previous: Deputy Commissioner, Executive Director at ICO (to 2022)	29 Sept 21
29	Maria Luisa Stasi	CSO/ academia	Article 19	Senior Legal Officer		12 Oct 21
30		Regulator				12 Oct 21
31		Government				12 Nov 21
32	Kate Brand	Regulator	CMA	Director of Data Science		15 Nov 21
33		Regulator				16 Dec 21

Published by
Alexander von Humboldt Institute for Internet and Society

in cooperation with
CREATe
R&I IN3 Internet interdisciplinary Institute Universitat Oberta de Catalunya
cnrs centre internet et societe
University of Tartu Johan Skytte Institute of Political Studies