

Student working paper series

Political misinformation in the UK

How to regulate political advertising and campaigning, especially regarding the risk of misinformation in social media, to provide a safe online space and upholding free speech?

Kai Foerster, MDS 2023

Angela Duarte, MDS 2023

Luis von Ingersleben, MPP 2023

Danayt Bokrezion, MPP 2023

11 May 2022

Political advertising on social media has influenced major historical events, like the Brexit referendum and the management of the ongoing COVID-19 pandemic. The United Kingdom (UK) government recognised the increasing threat that political misinformation poses and released its first draft on the Online Safety Bill (OSB) as a response. Ultimately, the bill is supposed to regulate political misinformation and turn Britain into “the safest place in the world to be online”. This paper aims to support the current draft of the OSB based on 10 recommendations. These highlight the necessity of avoiding ambiguity in the wording of the bill, guaranteeing the independence of Ofcom as a regulator, and reframing the Bill so that it recognises collective harm and the danger that political mis/disinformation can cause to democracy in the UK. We believe that our recommendations have the potential to significantly increase the impact of the current proposal.

Table of content

Table of content	2
1 Introduction	4
2 Background	4
2.1 <i>Misinformation and the Brexit referendum</i>	4
2.2 <i>Misinformation during the COVID-19 pandemic</i>	5
3 Policy Problem and Path.....	6
3.1 <i>A brief definition of misinformation and disinformation</i>	6
3.2 <i>Problems and drivers</i>	7
3.3 <i>Previous regulatory efforts</i>	8
3.4 <i>The newest approach to online harms in the UK: The Online Safety Bill (OSB)</i>	10
4 Actors	11
4.1 <i>Political parties</i>	12
4.1.1 <i>Conservative Party</i>	13
4.1.2 <i>Labour Party</i>	13
4.1.3 <i>Other parties</i>	13
4.2 <i>Nadine Dorries – Conservative Party</i>	14
4.3 <i>Damian Collins – Conservative Party</i>	14
4.4 <i>Joint Select Committee on the Draft Online Safety Bill</i>	14
4.5 <i>Lords Select Committee on Democracy and Digital Technologies</i>	15
4.6 <i>Office of Communications (Ofcom)</i>	15
4.7 <i>Other potential regulators</i>	16
4.7.1 <i>Advertising Standard Authority (ASA)</i>	16
4.7.2 <i>Electoral Commission</i>	16
4.7.3 <i>Financial Conduct Authority (FCA)</i>	17
4.7.4 <i>Police</i>	17
4.7.5 <i>Information Commissioners Office</i>	17
4.7.6 <i>UK Statistics Authority</i>	17
4.8 <i>Large social media platforms and technology companies</i>	17
4.9 <i>Companies making money from micro-targeting ads</i>	18
4.10 <i>Media actors</i>	18
4.11 <i>Civil Society Actors</i>	18
4.12 <i>Financial sector / City of London</i>	19
5 The Policy Design of the OSB	19
5.1 <i>The approach to harmful content online in the OSB: "Duties of Care"</i>	20

5.2	<i>Main policy instruments proposed in the Online Safety Bill (OSB)</i>	22
4.2.1	Regulatory instruments	22
4.2.2	Financial incentives	23
4.2.3	Information-based instruments	24
5.3	<i>Potential unintended effects of the OSB: a free pass to political advertising?</i>	25
6	Weaknesses, loopholes, ambiguities	26
7	Recommendations	28
8	Conclusion	30
	References	32

1 Introduction

The influence of social media platforms and tech companies like Facebook, Google and Instagram on people's everyday lives has rapidly increased throughout the past decade in the United Kingdom (UK). Likewise, the internet has grown to become the UK's second largest medium to stay up to date with the news. More than 70% of all UK citizens state that it is their main medium to consume news. Furthermore, recent studies found that approximately half of the British public obtains most of its news through social media. These numbers demonstrate the influence social media platforms have on UK citizens' everyday lives (Ofcom a, 2021).

The recent spike in digital news consumption has led to an increase in the connectedness of internet users, while also improving the accessibility of news and information for the broader public. However, not all information circulating on the internet is true. One fourth of UK citizens who use the internet claim to come across fake news about the coronavirus multiple times a week. Moreover, 24% of online users in the UK report to see the same false or misleading information two to four times a day. Alarming, this is only the percentage of misinformation that gets recognised by social media users. Historical political decisions and events like the Brexit referendum in 2016 and the crisis management during the ongoing COVID-19 pandemic have been heavily influenced by misinformation fluctuating around various social media channels (Ofcom b, 2021).

The lack of regulation, especially with respect to political misinformation, is still a problem in the UK. This paper aims to analyse the current draft of the Online Safety Bill (OSB), and the way it aims to regulate political misinformation through digital advertising. The analysis consists of three sections: one highlighting the current state in the policymaking process, one analysing all actors and players involved and one discussion the current draft of the bill. From this, we derive a series of current weaknesses and ambiguities of the draft bill which will be the basis of our recommendations.

2 Background

2.1 Misinformation and the Brexit referendum

Several academic analyses have shown that the successful 'Leave' campaign, which was promoted by EU-opponents, made use of new digital technologies like social media bots, mass data harvesting and targeted ads to influence peoples' opinions and spread far-right disinformation. These false or at best misleading narratives were picked up by many people online which led to its quick and unstoppable spread throughout the UK (Brändle, 2021). Some of the most compelling narratives which the Vote Leave campaign pushed were the following:

- The money saved from leaving the EU will result in the NHS getting £350m a week.
- Turkey is going to join the EU, and millions of people will flock to the UK.
- A free-trade deal with the EU will be 'the easiest thing in human history'.
- "Brexit does not mean the UK will leave the single market" (The Independent, 2018).

The first two messages were especially widespread, even though they were proven to be wrong.

Misinformation during elections and referendum campaigns is not a new tactic of political campaigning. The big difference is the ease with which it spreads on digital social platforms. Most of the Leave campaign's financial resources were allocated on direct digital communications, which led to them to spread nearly a billion targeted digital ads in favour of their Leave Campaign until the referendum date (Marshall & Drieschova, 2018). Further analysis proved that social media users with Eurosceptic opinions, mostly supporting the Leave campaign, were generally more active, vocal and numerous than Remain supporters. They were also less open for other options and more likely to be found in echo chambers. These echo chambers emerged in homogeneous spaces like Facebook groups, where like-minded people were only among themselves. There was generally more Eurosceptic online content during the time leading up to the referendum, which was supported by a press coverage that predominantly favoured the Leave campaign. Additionally, the average UK citizen was also more likely to encounter Eurosceptic content offline. However, the big difference between social media and broadcast and print media was the fact that social media remains to be insufficiently regulated. This enabled misinformation and disinformation to spread more easily and rapidly (Hänska & Bauchowitz, 2017).

2.2 Misinformation during the COVID-19 pandemic

A more recent demonstration of the dangers of political misinformation on social media is its continuous spread during the ongoing COVID-19 pandemic. There have been multiple cases of online misinformation. However, this analysis will focus on the illustration of one specific case, which clarifies the current dangers of social media misinformation in comparison to disinformation on national TV. On 8 April 2020, the local TV channel London Live featured a talk show called 'London Real' hosted by a moderator called Brian Rose. Rose's guest, former football and sports broadcaster David Icke, made multiple false claims about the virus and its spread. The Office of Communications, the UK's national media regulatory authority, which is also known as Ofcom, received several complaints from viewers of the show. Ofcom then identified multiple false claims, which could potentially harm the viewers of the show. These included "health claims related to the virus which may be harmful; medical advice which may be harmful; and accuracy or materially misleadingness in programmes in relation to the virus or public policy regarding it" (Ofcom c, 2020, 1). As a result, the owner of the TV station ESTV Limited, which owns London Live, was sanctioned by Ofcom. The national authority justifies this sanction with the concern that the content broadcasted in the show could significantly harm viewers during the crisis. However, similar content continues to circulate freely on social media platforms (Allington et al, 2020).

Scholars from Oxford University and the Reuters Institute published a joint research paper in which they analysed the different sources, types and claims of misinformation that is related to the COVID-19 pandemic. The study analysed 225 pieces of misinformation in the UK which have been detected as false or misleading by fact checkers. Most of the misinformation analysed in the paper consists of a mixture of true information and false narratives, which have been spun into false claims with some true backgrounds. They detected that 87% of the misinformation circulation on social media is based on reconfigured true facts, while about 12% of the misleading content is based completely on lies. Public figures, politicians and celebrities like David Icke and Brian Rose are only

responsible for about 20% of misinformation, although they simultaneously accounted for 69% of the engagement around fake news on social media. This shows that most of the false narratives are spun by a few people and then multiplied heavily by many smaller accounts, with less engagement (Brennen et al, 2020).

The study was able to detect a positive association between beliefs of false news about COVID-19 and the use of social media as a source of information. The effect is the strongest for Facebook, Twitter and YouTube, with YouTube being the worst. This is a new dynamic which has started with the rise of social media. Significantly more people have the possibility to produce, transfer and duplicate misinformation while there is also a significant decrease in the fact-checking of the produced information (Brennen et al, 2020). This can be dangerous and will be further elaborated in the analysis of the problems and drivers.

3 Policy Problem and Path

3.1 A brief definition of misinformation and disinformation

Political misinformation is defined as information on a topic that is false but not created to cause harm. The sender of misinformation is not aware that the information is inaccurate and spreads it with good intention. The distinction with disinformation can be drawn at the point where an intent comes into play.

Political disinformation is defined as false information that is being created with the intention to harm an individual, institution or discourse. The person disseminating information is aware of its inaccuracy and deliberately decides to spread it. Common motives for spreading disinformation are the desire to exert or increase political influence or the intention of creating pointless confusion (Wardle, 2019).

Regardless of malicious intent, holding and spreading inaccurate political beliefs has the potential to destabilise democratic institutions and the political system itself, as knowledge about political events and the political system more generally is considered the basis of popular support for democratic principles and therefore, as the foundation of representative democracy (Galston, 2018).

There are different explanatory approaches for political misinformation and why people keep consuming it. One of the more common reasons lies in the “psychological architecture” an individual utilises when thinking about a particular topic. There is a general human motivation to strive towards a particular end or goal, and this tendency influences the entire thought process from the type of information sources considered to the implications drawn from that information (Turcilo & Obrenovic, 2020).

The socioeconomic trend of using social media as a main source of information has added to this tendency as people often stay within their opinion groups, where the alleged truth is set in echo chambers through mutual assurance and where one-sided news are used to

reiterate existing sentiments. This feeling of “tribe-like” connection to a certain group is exemplary for people sharing misinformation (Jerit & Zhao, 2020).

3.2 Problems and drivers

The first step to elaborate adequate measures against misinformation through political advertising is to take a closer look at the actual roots of misinformation and the different stakeholder groups involved in the topic in the UK.

First, the rapid evolution of the digital landscape opens new possibilities for the spread of misinformation through cheap, far-reaching technologies in advertising on social media. Brexit showed the efficacy of manipulating voters through micro-targeting and concerted disinformation campaigns. However, that’s only the tip of the iceberg: deepfakes, “coordinated inauthentic activity” as Facebook calls the united threat of bots and fake accounts, can be used by politically motivated groups and politicians to “confuse the information environment” and undermine trust in the institutions and academic research in the case of the pandemic (Constitution Unit, 2021).

Second, there is very little transparency in the field of political advertising and online campaigning in the UK. Although this fact has been discussed after Brexit, there is no policy regulating it. This is partly caused by the fact that political figures have incentives to use and profit from political disinformation through digital campaigning. As further elaborated in Section 3, they have a strong incentive to weaken laws addressing the topic.

Third, large parts of the public are aware of the amount of misinformation/disinformation circulating on social media. They know that there is no barrier to produce and reproduce false news, but it is often difficult to distinguish between news that have been fact-checked and fake news. Also, some citizens might mistrust the government and institutions and quickly believe in “alternative world views.” These reasons make the public more prone to consume false and misleading information. Essentially, the problem is that the public is not trained enough to evaluate and produce online content and is not aware enough of its responsibilities as digital citizens.

Moreover, distrust resulting from the spread of misinformation has negative consequences for many other stakeholders. For example, misinformation’s frequent discrediting of news and research outlets has led to distrust towards all news circulating on the internet. Furthermore, politicised outlets that are very active in campaigns and present themselves as investigative journalism erode the credibility of journalism and fact-checking. This has made “alternative” sources of information more appealing.

Finally, misinformation and disinformation has been called a threat to democracy (The Constitution Unit, 2021). Tech companies such as Facebook or Twitter decide which content will be viewed by the public through their algorithms. They actively influence newsfeeds, which can ultimately sway political discourse and votes. The Brexit referendum and the amount of distrust of the COVID-19 vaccine were only two examples which demonstrate this. Previous debates, however, proved that a lack of moderation in the field of harmful content, including misinformation through political advertising, has led to major public outcries against those companies.

All in all, these five problems with their respective drivers add up into a unified policy problem: despite suffering from the consequences of mis/disinformation spread through digital political advertising, the UK has no clear regulation of this phenomenon. Since the stakes are so high and mis/disinformation efforts can lead to harmful content online, efforts related to the regulation of harmful content online can provide an opportunity of regulating mis/disinformation through political advertising. The extent to which they do will be discussed in the next section.

3.3 Previous regulatory efforts

The problems described above demonstrate some of the biggest challenges that can result from the lack of misinformation regulation on social media. There have been a range of regulatory and voluntary initiatives aimed at addressing these problems since 2017. However, recurring crises like the spread of misinformation during the Brexit vote or the COVID-19 pandemic prove that previous regulations were not stringent enough to keep UK users safe online.

The first symbolic government step to increase regulation of social media platforms and providers of internet services was the publication of the green paper with an 'Internet Safety Strategy' in 2017. The paper proclaimed the government's goal to "Make Britain the best place in the world to setup and run a digital business, while simultaneously ensuring that Britain is the safest place in the world to be online" (Green paper, 2017, 3). Enforcement of that goal was then planned to be based on three objectives, on which the paper was based. It wanted to make sure that:

- "What is unacceptable offline should be unacceptable online;
- All users should be empowered to manage online risks and stay safe;

Technology companies have a responsibility to their users" (Green paper, 2017, 3).

The paper was the outcome of the government's consultation with online safety organisations and charities, academics and large tech companies. They developed a series of strategies, including:

- "The introduction of a social media code of practice, transparency reporting and a social media levy,
- technological solutions to online harms,
- developing children's digital literacy,
- support for parents and carers,
- adults' experience of online abuse, and
- young people's use of online dating websites/ applications" (Department for Digital, Culture, Media & Sport, 2017, 3).

However, the most important takeaway for the fight against misinformation on social media in the UK is that the green paper did not address its specific harms. A deeper analysis of the paper shows that the term 'misinformation' was not mentioned once. It rather relies on very general terms like 'illegal content' or 'harmful content' and fails to address the specific dangers posed by misinformation on social media and more specifically, misinformation in political advertising or health matters. The green paper was only a first draft on the road to the OSB, which will be discussed in greater detail later.

After a consolidation phase, an updated version of the green paper called the “Online Harms White Paper” was published in 2019. The overall goal of making the UK “the safest place in the world to be online” remained the same but the wording and approach became clearer. The underlying strategic aims of the white paper were:

- “A free, open, and secure internet,
- freedom of expression online,
- An online environment where companies take effective steps to keep their users safe, and where criminal, terrorist and hostile foreign state activity is not left to contaminate the online space,
- Rules and norms for the internet that discourage harmful behaviour
- The UK as a thriving digital economy, with a prosperous ecosystem of companies developing innovation in online safety,
- Citizens who understand the risks of online activity, challenge unacceptable behaviours and know how to access help if they experience harm online, with children receiving extra protection,
- A global coalition of countries all taking coordinated steps to keep their citizens safe online,
- Renewed public confidence and trust in online companies and services” (Department for Digital, Culture, Media & Sport, 2019, 6).

Unlike the green paper, the white paper did recognise the dangers of the spread of fake news online. The term ‘disinformation’ was used 38 times in the paper highlighting the need for policies that address the danger it poses. Political misinformation and political advertising on social media were mentioned a couple of times. Nevertheless, the paper failed to address either of the topics concretely and therefore also did not outline relevant regulatory frameworks. As the next and crucial step of the law-making process, the white paper was transformed into a draft of the OSB this year, which will have its first reading in Parliament by March 2022 and will be the central focus of this paper.

However, there is also another side to the regulation of social media companies with respect to misinformation and political advertising. The previous efforts mentioned above are also the result of inadequate existing mandates regarding the statutory processing of political advertising.

Since 2003, all political advertising has been banned from radio and television as part of the Communications Act. Since then, “political advertisement” includes all efforts to promote governmental actions, influence legislative decision-making and campaigning for the efforts of political parties (Parliament of the United Kingdom, 2003). The Communications Act also stipulates that Ofcom is responsible for overseeing and enforcing the law.

Political parties are granted the opportunity to use specific political airtime in the build-up to elections. This law stems from a time when broadcasting, via radio and television, were the main channels for political communication. In addition, parties and their campaigners have a fixed budget for advertising during elections and referendums.

Moreover, advertising in general is regulated by the Advertising Standards Authority (ASA), but political advertising is specifically exempt from the ASA's supervision due to concerns about the ASA potentially limiting freedom of speech.

Money spent on digital political advertising has steadily increased over the past years from 0.3% (2011) to 42.8% (2017) of the total advertising budget (The Electoral Commission, 2018). This share does not include the possibility for political parties to contact potential voters for free on social media. The Electoral Commission published recommendations on how to regulate this type of content in 2018, which included giving the Commission greater executive rights to request data from third-party operators and digital watermarks for campaign materials. The proposal was seen as the effort to emulate the offline law for regulating advertising via broadcast.

The given recommendations have not been adopted by lawmakers to increase transparency for authorities and voters. Instead, different platform providers and tech companies have started to oblige to different standards, for example Facebook offering an inventory of all ads being visible on their platform. (House of Commons Library, 2019).

As the UK government initially hesitated to further address political advertising, multiple studies and reports were released in 2019 by the House of Commons and the Media and Sports select committee that proposed changes to the electoral system.

A second legislative effort was started with the release of the "digital imprints" consultation, which aimed to increase transparency and trust in the UK democracy by obliging political campaigners to explicitly state who they are and whose content they are promoting (Cabinet Office, 2020). Even though a required imprint for digital content is viewed as an important step, there was still disappointment across different actors that the consultation did not include any planned efforts to assess the accuracy of digital political content.

3.4 The newest approach to online harms in the UK: The Online Safety Bill (OSB)

The OSB is the draft currently under pre-legislative scrutiny in the UK. It aims to make "the internet a safer place for all" (DCMS, 2021c) by addressing illegal and harmful content online, including mis/disinformation (DCMS, 2021b, 2021c).

To achieve this goal, the OSB creates a new regulatory regime by imposing duties of care to internet services with the specific intent of protecting users and their rights to freedom of expression and privacy (DCMS, 2021b).

At the front and centre of this regulatory regime is Ofcom, an organisation independent of the government and financed by the regulated companies (Ofcom c, 2021). Ofcom will oversee and regulate internet services and will implement the UK's media literacy strategy¹ (DCMS, 2021a).

¹ The first line of the draft bill reads: "Make provision for and in connection with the regulation by Ofcom of certain internet services; and to make provision about and in connection with Ofcom's functions in relation to media literacy." (OSB, 2021). Ofcom's duties are discussed in four of the seven sections of the draft bill (Freemont, 2021). In this paper, Ofcom's role regarding the regulation of political advertising will be discussed in section 3: actors and its powers will be discussed in the Policy Instruments Section.

Although the draft bill does not explicitly mention the main objectives of such a regulatory regime, they appear on the impact assessment presented to the Regulatory Policy Committee, as follows (DCMS, 2021c):

1. Improving the safety of users online by reducing the incidence of specific online harms, especially those who affect specific vulnerable groups.
2. Preserving freedom of expression of UK citizens through safeguards, such as collecting and reporting transparency data.
3. “Improving the efficacy of law enforcement and crime prevention with respect to illegal content and behaviour online” (DCMS, 2021c)
4. Increasing the efficiency, coherence, and clarity of governmental activity tackling online harms and empowering users to stay safe online.
5. Creating a culture of transparency, which enhances the amount and quality of information related to online harms available in the UK.

Political advertising in social media is not explicitly mentioned in the draft bill nor in the explanatory notes. However, it is at the intersection of the first two objectives of the OSB: while political advertising might be the vehicle of online harms through its spreading of mis/disinformation, it is also a form of expression that might need protection so that parties, especially the smaller ones, can make their platforms known in the online playing field. The OSB can address some of the risks and needs of political advertising. However, the lack of specific provisions regarding this issue in the draft bill can have unintended consequences on the regulation of misinformation through political advertising in social media.

4 Actors

As discussed in the previous section, the OSB which is regarded as the main legislative proposal to regulate misinformation is in the draft stage. The draft bill stage provides a unique setting for public consultations and lobbying because decision-making is concentrated to two authorities: the government that produces the draft bill and the Parliament’s select committees that scrutinise the proposal made by the government (UK Parliament, n.d.).

The government is represented by Nadine Dorries who is currently Secretary of State for Digital, Culture, Media and Sport and responsible for drafting the bill. The key decision-maker in Parliament is Damian Collins, the chair of the Joint Committee on the Draft Online Safety Bill, who is currently scrutinising the bill. Throughout the drafting process, it is common practice that draft bills and white papers are open to public deliberation in so called public consultations (GOV.UK, 2019a). The select committees also invite representatives from different interest groups during the consultation stage which opens the doors for business actors, civil society actors and other actors to take part in the deliberation (UK Parliament, n.d.).

This paper identifies the following categories of actors represented below in the power vs. interest grid (Figure 1) as suggested by Ackermann and Eden (2011). Due to the complexity of the actor relationships, the power-interest grid represents actors grouped together in categories apart from a few exceptions. Over the course of this section, the actor categories

are disaggregated into specific institutions and individuals and described in more detail. Finally, the actors presented in this chapter are summarised in the more detailed power-interest grid (Figure 2, page 20) which the reader will be able to appreciate and understand by the end of this section.

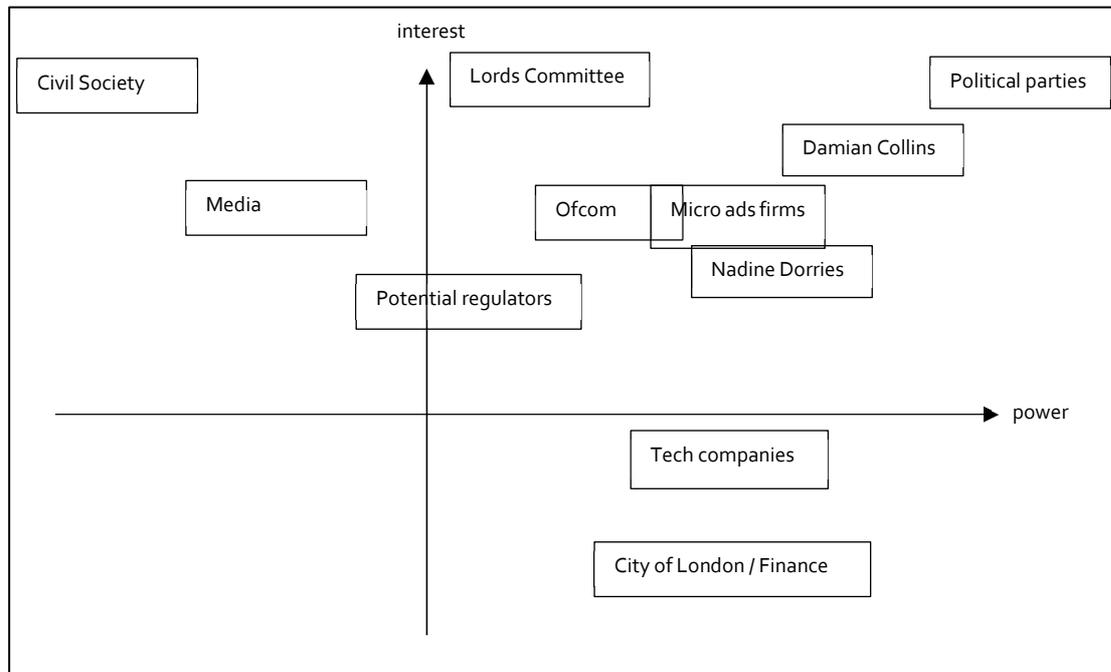


Figure 1: Power-interest grid

As further discussed below, Figure 1 highlights that the UK political parties, who have the most power in the decision-making process, are also the ones who have a strong interest in excluding regulation on political advertising in the OSB. In contrast, civil society actors, the media, independent regulators and even tech companies are not opposed to the inclusion of political advertising regulation. In a nutshell, the key takeaway of the actor analysis is that political parties must be persuaded to regulate political advertising. This will require independent regulators, the media, civil society and the private sector to work together to put the debate on regulating political advertising back on the agenda. This coalition must frame the absence of regulation as threatening democracy and pressure the government and Parliament to include tighter measures on political advertising to “save” the UK democracy.

The next sections disentangle the role, interest and power of each actor involved in the policy process in more detail.

4.1 Political parties

The two dominant political parties in the UK are the Conservative Party and the Labour Party. The antipathy towards regulating political advertising is shared by the Conservative Party, the Labour Party and the Liberal Democrats. Most of what applies to the Conservative Party and Labour Party reflects the stance of other political parties, mainly the Liberal Democrats, too.

4.1.1 Conservative Party

The ruling party in the UK, the Conservative Party is in government and has a majority in Parliament. Therefore, this party not only has the power to draft bills but to pass and veto them in Parliament. As it stands, with a majority of 361/650 seats in the House of Commons, no law can pass without the support of the Conservative Party (UK Parliament, n.d.). The Conservative Party is led by Boris Johnson who is also the Prime Minister of the UK.

The Conservative Party is opposed to any kind of regulation on political advertising, especially with respect to the truthfulness of the advertising content on social media. It has actively used political advertising on social media in the 2019 election and has been experimenting with different ads to reach different socio-demographic groups (First Draft, 2019). The Conservative Party spent the most out of all parties on advertising via Facebook and Instagram preceding the 2019 general election (Barton et al., 2019). Truthfulness was not a priority in these ads as Dotto (2019) from First Draft, an NGO, documents. A research paper from 2013 further shows that Conservative politicians were not averse to local political marketing using different kind of media either (Reeves, 2019).

Hard-line Brexiteer and leading libertarian Tory MP David Davis has framed the current draft bill (OSB) as “catastrophic for free speech” even without any additional regulation for political advertising (Tambini, 2021). It is therefore unlikely that the Conservative Party will back an amendment including regulation for political advertising, especially when it comes to limiting the content of political advertising.

4.1.2 Labour Party

The Labour Party is currently the main opposition party in the UK. In this role, it scrutinises the actions and legislative proposals made by the Conservative Party. However, having only 199/650 seats in the House of Commons, even in a coalition with all other opposition parties the Labour party could not veto any law and is therefore limited in terms of political power (UK Parliament, n.d.). The Labour Party is led by MP Keir Starmer.

The Labour Party is likely not interested in regulating political advertising either. In fact, its manifesto for the 2019 election does not mention political advertising even once (Labour Party, 2019). They have also used misleading political advertising during the 2019 general elections to win votes. For example, ex-Labour leader Jeremy Corbyn famously claimed that Boris Johnson was planning to privatise the NHS which turned out to be false (Tidy and Schraer, 2019). The Labour Party spent about 88,000 pounds on political advertising on Facebook, second after the Conservative Party. A digital campaign guide found on the internet from the Labour Party specifically urges members to use social media posts with flashy, short messages to win votes (Labour Party, 2019). All this evidence underlines that the Labour Party is likely not interested in regulating political advertising online as it is a beneficiary of the current loose regulations.

4.1.3 Other parties

All other parties, such as the Liberal Democrats, have far fewer seats in the House of Commons and are unlikely to exert great influence on the bill. However, it should be noted

that the Liberal Democrats have been actively publishing misleading infographics to convince the electorate to vote for them in the 2019 general elections. Therefore, they are likely to be part of the problem rather than the solution when it comes to proposing regulation against misleading political advertising on social media (Schraer, 2019).

4.2 Nadine Dorries – Conservative Party

Nadine Dorries is Secretary of State for Digital, Media, Culture and Sport since the cabinet reshuffle in September 2021. As the head of the department in charge of drafting the OSB, she has a lot of influence on the content of the bill. She has stated that she is overhauling the draft to make it stronger (Dickson, 2021).

She is known as loyal Boris Johnson and has been criticised in the media for her aggressive tone toward “left snowflakes” on social media who she believes should be “tone[d] down” (Stone and Woodcock, 2021). Dorries grew up in one of the most deprived areas of Liverpool and has made it her mission as secretary to make the OSB “much tougher and stronger” to protect against abuse and harassment (BBC News, 2021). She has not been vocal about adding political advertising on the OSB and is likely to endorse her party’s line on the issue.

4.3 Damian Collins – Conservative Party

Damian Collins is the Conservative MP for Folkestone and Hythe and Chair of the Joint Committee on the Draft Online Safety Bill. Given the committee is scrutinising and reporting back to the Department for Digital, Media, Culture and Sport for possible amendments right now, he has a strong influence on the direction of the bill (UK Parliament, n.d.).

Collins has experience in social media regulation and sees political disinformation as a big issue that must be solved. Since 2010, he has been member of the House of Commons Culture, Media and Sports Select Committee. He launched the inquiry on disinformation against Cambridge Analytica and was the initiator of a global conference devoted to discussing issues concerning disinformation in 2018. He supports reforms to UK election law to apply to online content as it applies to offline content. He has advocated for misleading campaign videos to be flagged as harmful content on social media (Wikipedia, 2021). Therefore, he is likely to endorse amendments to regulate political advertising online.

4.4 Joint Select Committee on the Draft Online Safety Bill

Chaired by Collins, this joint committee includes members of the House of Commons and the House of Lords that scrutinise the current draft of the OSB. The committee has twelve members, six of which are from the House of Commons and the other six from the House of Lords. Surprisingly, the committee includes Lords who are not part of the Select Committee on Democracy and Digital Technology which spearheaded regulating of social media through its report on the effect of digital technologies on the UK democracy in June 2020 (UK Parliament, n.d.).

It is difficult to predict the committee’s stance towards regulating online political advertising with respect to disinformation. In the report that was published on 13 December

2021, the committee did not include their view on the issue and thereby set the agenda for political advertising to be excluded from the bill. One must weigh the MP's party interest that opposes intervention into political advertising against the scepticism of the members of the committee from the House of Lords, who are less dependent on their affiliated political party. Furthermore, Collins' vocal criticism against election fraud and disinformation might affect the committee's conclusion on how the draft bill should be amended. It is unlikely that the committee will push for the inclusion of political advertising. However, it has recommended the addition of paid-for advertising to be covered by the bill (UK Parliament, 2021).

4.5 Lords Select Committee on Democracy and Digital Technologies

The Lords Select Committee on Democracy and Digital Technologies was appointed on 13 June 2019 with the purpose of inquiring into the threat that digital technologies pose to the UK democracy (UK Parliament, n.d.). Their main report was published on 29 June 2020 under the name "Digital Technologies and the Resurrection of Trust" (House of Lords, 2019). It has been very influential since it covers a broad range of threats and possible solutions. Some of the Lords in the committee also serve as members of the Joint Committee on the Draft Online Safety Bill (Constitution Unit, 2020).

The Lords Committee urges online political advertising to be regulated and fact-checked to avoid the spread of disinformation and misleading information by political parties during election campaigns. The report clearly outlines the threat that online political advertising poses to the UK democracy by eroding trust in political parties who too often spread misleading information and disinformation during election campaigns. The committee highlights the fact that regulation of political ads will require collaboration from the political parties. It notes that none of the current regulators has the appetite or the resources to regulate political advertising (House of Lords, 2019).

4.6 Office of Communications (Ofcom)

As outlined in the previous section political advertising is prohibited in the UK on broadcast media including TV and radio (ASA, n.a.). Ofcom is responsible for the application of this rule. However, as further described below, political advertising on non-broadcast media including social media is currently permissible.

As already mentioned, Ofcom will also be the regulator of social media platforms and providers of internet services according to the draft of the OSB. Dame Melanie Dawes, chief executive of Ofcom, told the BBC that their agency was motivated to take up the new role, albeit having to build up a team that would be able to cope with the amount of complains and legal backlash by providers of internet services (Wakefield, 2021).

Ofcom has positioned itself as moderately concerned about the proliferation of disinformation in political campaigning. In a recent study in collaboration with Facebook and Google, Ofcom explores how self-regulation worked in practice and recommends more transparency and handholding for tech companies to effectively regulate misinformation on social media platforms (Ofcom c, 2021).

4.7 Other potential regulators

To cooperate on future regulation of political misinformation, the Digital Regulation Cooperation Forum was established in March 2021. It consists of the Competition and Markets Authority, Ofcom, the Information Commissioner's Office and the Financial Conduct Authority (GOV.UK, 2021). The forum has been regarded as a key step to close loopholes in online regulation and could function as a joint regulator for online political advertising in the future (Parliamentlive.tv, 2021). This is because the responsibility to regulate misinformation is currently split between different regulators in the UK. All regulators cautiously point towards the harm that misinformation in political advertising is causing, albeit being careful not to condemn the political parties for spreading fake news.

The overview of the main regulators below brings together their functions and perspective on regulating political advertising. It highlights the fragmentation of the regulatory landscape in the UK which is deemed to be one reason misinformation in political advertising has not been effectively regulated so far.

4.7.1 Advertising Standard Authority (ASA)

The ASA regulates commercial advertising in the UK. In partnership with businesses, it thoroughly assesses ads for accuracy. The scope of the ASA includes online advertising as well as online behavioural ads, also known as micro-targeted ads (ASA, n.a.). According to the UK Code of Non-broadcast Advertising, Sales Promotion and Direct Marketing (CAP Code), political advertising has been exempt from the CAP code since 1999. However, advertising created by the government which is not part of an election campaign is subject to regulation by the ASA (Electoral Commission, 2021).

The ASA has positioned itself in favour of further regulation of political advertising online (ASA, 2020) but does not see itself as a future regulator of political advertising. Instead, it has called for an alliance of regulators to address misinformation in political advertising and reiterated that regulation of political advertising will require the support of the political parties themselves (House of Lords, 2019). The ASA has noted that it considers political advertising a sensitive topic and voiced its concerns about potential threats to its reputation if it were to take up the responsibility of regulating it.

4.7.2 Electoral Commission

The Electoral Commission is an independent body that oversees elections and election finance in the UK (Electoral Commission, n.a.).

As previously mentioned, the Electoral Commission positions itself strongly against misleading political advertising online and has called for more regulation. In a recent report assessing the 2019 general elections, the Electoral Commission warned "misleading campaigning techniques [that] risk undermining voter's trust", especially on social media. The Commission has called the current rules for campaigning to be updated to the digital age (Electoral Commission, 2019).

4.7.3 Financial Conduct Authority (FCA)

The FCA is responsible for combatting financial fraud and protecting consumers from financial scams (FCA, 2016). Therefore, it is responsible for any misleading advertising that concern financial involvement, whether online or offline. The FCA has been lobbying for financial scams to be included into the scope of the OSB (FCA, 2020).

4.7.4 Police

The police are responsible for any false statement made on any political advertisement concerning a person's action or character (Electoral Commission, 2021). The police have never issued an official statement on the matter of misinformation in political advertising.

4.7.5 Information Commissioners Office

The Information Commissioners Office is responsible for any privacy breach online. Privacy is deeply intertwined with micro-targeted ads, which make use of personal information gathered through cookies and online profiles to target specific ads to people (ICO, n.a.). While the Information Commissioners Office is likely to endorse further regulation of political advertising, no official statement on the matter has been found.

4.7.6 UK Statistics Authority

The UK Statistics Authority regulates the quality and misuse of statistics, especially those that are concerned with the social, economic and political matters (UKSA, n.a.). The authority is the point of contact if a statistic in a political ad is misleading or false (Electoral Commission, 2021). Likewise, while the UK Statistics Authority is likely to reiterate the importance of truth in political advertising, no official statement on the matter has been found.

4.8 Large social media platforms and technology companies

Large social media platforms and tech companies including Facebook, Snapchat and Google have reacted to public outrage of the recent years and begun making political advertising transparent on their platforms. Now, it is possible to track on their transparency websites who paid how much for which ads (see: Facebook, n.a., Google, n.a., Snap, n.a.). Twitter has gone as far as to ban political advertising on its platform all together (Twitter, n.a.).

In a written statement to Parliament, Twitter has lobbied for more clarity on the definition of content that will be taken down in the future by Ofcom. Particularly, Twitter worries that journalistic content protected by the bill to uphold freedom of speech could be misused to spread disinformation during political campaigns (UK Parliament, n.d.).

Overall, tech companies seem to cautiously endorse further regulation of online content, including proposals made in the OSB (Tambini, 2021). Therefore, they can be expected to support further regulation on political advertising too if it gets incorporated in the OSB.

4.9 Companies making money from micro-targeting ads

Companies selling their services to produce micro-targeting ads such as AggregateIQ or Auspex International, the successor of Cambridge Analytica, are firms that use behavioural advertising techniques to target individual consumers with “more persuasive” individualised ads (Auspex International, n.a.). However, there is no evidence from academic research so far that the targeted nature of the ads actually makes them more persuasive according to experts interviewed by the Lords Select Committee (House of Lords, 2019).

Political parties in the UK have attempted to increase the effectiveness of their political ads through micro-targeting. Firms selling such services are keen on keeping the political advertising landscape unregulated and have no interest in exposing the fact that the effectiveness of their ads may be smaller than conventionally thought of (House of Lords, 2019).

4.10 Media actors

Key media actors including the BBC and the Guardian have grouped together under the “Coalition for Reform of Political Advertising” which lobbies for regulating dis- and misinformation online (UK Parliament, n.d.). The media has backed the draft OBS strongly, in particular on the issues of misinformation and harmful content.

Regulation of misinformation on social media is in the existential interest of media outlets as social media platforms are increasingly overtaking their role as news providers (Tambini, 2021). As one way to combat misinformation online, some media outlets provide their own fact-checking websites. For example, the BBC has its own fact-checker called BBC Reality Check (BBC Reality Check, n.a.). The media has been a key actor exposing the disinformation that political parties in the UK spread during the 2019 general elections and will likely lobby for the inclusion of regulation to fight disinformation in political advertising (Barton et al., 2019).

4.11 Civil society actors

Civil society actors including NGOs, foundations and academia have been advocates of stronger regulation against misleading content and disinformation in political advertising and campaigning.

For example, First Draft, an NGO backed by democracy advocacy foundations and tech companies exposed disinformation which spread in the 2019 general election and calls for a crackdown on harmful misinformation (First Draft, n.a.). Another organisation that has called for regulation on political advertising is Whotargets.me, which is backed by educational foundations and universities including the London School of Economics and Political Science and the Max Planck Institute (Whogets.me, 2021 & n.a.). While these organisations have extensive expertise in the field of political advertising and campaigning and its impact on election outcomes, they are not powerful politically speaking and will therefore unlikely affect the policy process without collaborating with more media and business actors.

4.12 Financial sector / City of London

The financial sector plays a large role for any policy in the UK, given its dominance (Hassel and Wegrich, forthcoming: 251), but it has held back its involvement on the question of political advertising. Yet, it is noteworthy that the financial sector has expressed a strong interest in adding online scam ads to the scope of the OSB (UK Finance, 2021).

The actors introduced above can be summarised in the more detailed power-interest grid which highlights that both main decision-makers at this stage are a part of the Conservative Party, a staunch opponent of regulation in this area. It will therefore require smart reframing to convince the political parties, especially the Conservative Party, to change their stance on misinformation in political advertising. Mobilising powerful private companies and public institutions such as the tech companies, the financial sector, and regulators to back the proposal of regulating political advertising in the OSB will also be necessary.

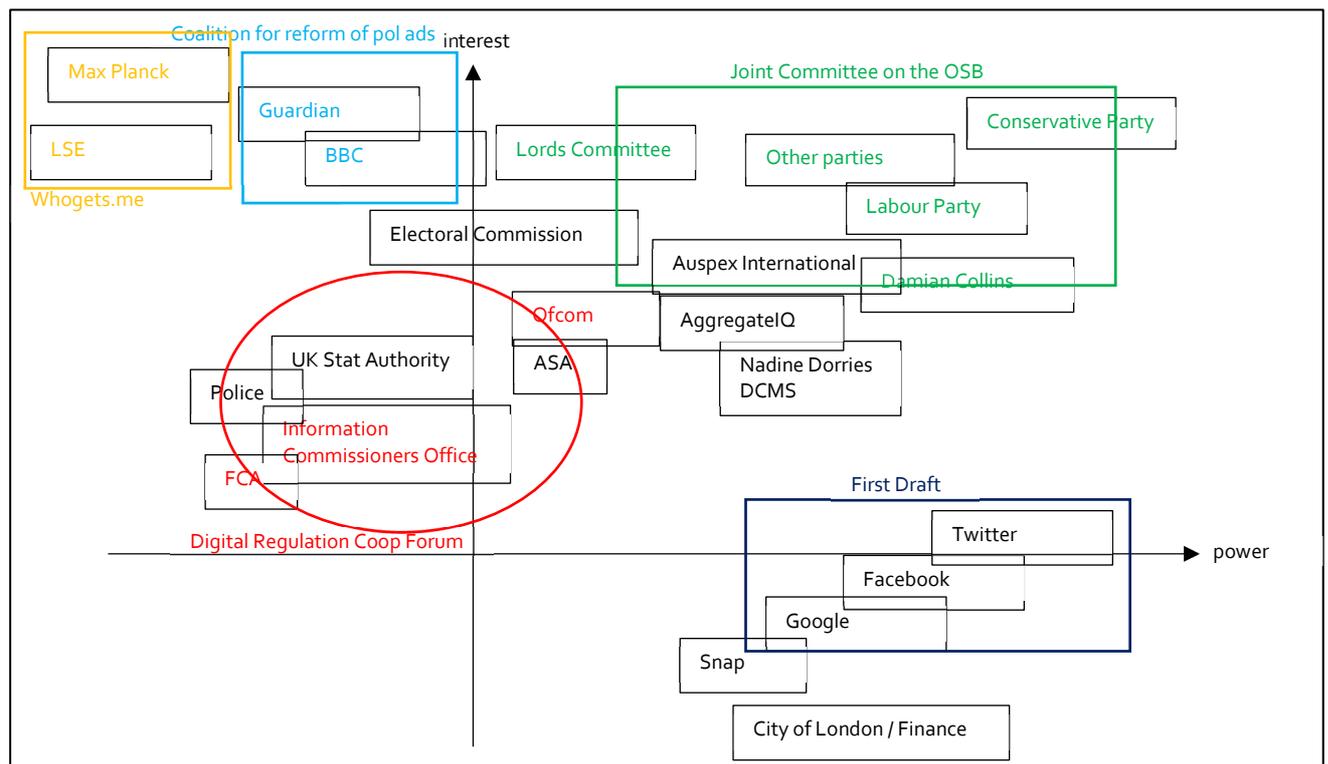


Figure 2: Power-interest grid (detailed)

5 The Policy Design of the OSB

The OSB strays away from the self-regulation of internet services, much like other regulations currently discussed: the DSA in the EU, the NetzDG in Germany, and the Avia Law in France. Since the Cambridge Analytica scandal, the tendency in Europe has shifted to a more regulatory, government-led framework in which specific agencies enforce and

oversee the regulation. In the UK, this change in the approach to internet services is not limited to online harms; regulatory efforts in privacy, data protection, competition and consumer protection also follow this trend (Woods, 2021).

This section briefly discusses how the OSB created a new regulatory regime for online harms. First, it recalls the approach towards illegal and harmful content online to analyse the main policy instruments proposed to address it in the second part. Finally, it outlines potential problems of these instruments, including some unintended consequences in the regulation of misinformation in political advertising.

5.1 The approach to harmful content online in the OSB: “Duties of care”

The OSB protects users through a responsibility framework that i) considers different types of online harms, ii) categorises internet services according to their size and level of risk, and iii) assigns to them differentiated duties of care, based on the categories mentioned above (Woods, 2021).

Regarding harmful online content, the OSB does not provide a comprehensive definition of “harm” caused by online content. This lack of clarity was already outlined in the Full Government Response (FGR) to the Online Harms White Paper (OHWP) (DCMS & Home Department, 2020). However, the Explanatory Notes to the OSB stress that future legislation must clarify the general definition of harmful content to better describe the scope of the policy – that is, which online contents and activities are covered by it (DCMS, 2021b).

Nonetheless, the OSB divides the idea of harmful content into three broad categories, which group together different kinds of online activity and material and allow for a more unified response. Although not explicitly mentioned on the draft bill, these categories are described in the impact assessment (2021) as follows:

1. Illegal content and activity (offences under the law, such as terrorism and child abuse).
2. Legal but harmful content and activity (not offences under UK law, but contents that can cause psychological or physical harms to adults of ordinary sensibilities, such as mis/disinformation).
3. User-generated content and activity which might cause psychological and physical harm to children, such as pornographic and violent content.

The OHWP included a more specific list of harms, such as harassment and cyberbullying, but it was not exhaustive (DCMS, 2021b). Although some of the harms listed by the OHWP fall within the above categories, potentially harmful content related to political misinformation, such as political advertising, microtargeting and concerted disinformation campaigns, do not appear to be within the scope of the OSB. This omission is surprising since a report produced by the Lords Committee on Democracy and Digital Technologies

(2020) explicitly mentions the urgency for “political advertising to be brought into line with other advertising in the requirement for truth and accuracy.”²

To tackle the outlined types of harmful content, the bill divides tech companies into providers of “search” and “user-to-user” services and assigns differentiated expectations and responsibilities to them. “Search services” correspond to search engines, which do not provide the possibility of user interaction; “user-to-user” services are those that allow users to encounter other users, as well as content generated, uploaded or shared by them (DCMS, 2021a).³

Additionally, online services will be divided into two categories according to threshold conditions to be determined by the Secretary of State and Ofcom based on the number of users, level of risk and other criteria deemed necessary by the offices.⁴ The FGR clarifies that most services will be “Category 2 services.” However, “high-risk, high-reach services will be designated as “Category 1 services:” it is generally assumed that the largest and most popular social media sites are “Category 1. User-to-user” services (DCMS et al., 2021). This categorisation of services aims to prevent disproportionate burdens on small businesses and make companies with large online presence accountable for their terms of use (DCMS & Home Department, 2020).

Finally, the OSB assigns differentiated duties to providers of internet services according to their category, the types of harmful content potentially circulating on their services, and whether they are accessible to adults or children (Woods, 2021). The following are summarised versions of the “duties of care”:

1. All providers must assess risks their sites may pose to the youngest and most vulnerable people and protect children from inappropriate content and harmful activity,
2. All providers must act against illegal content, which comprises crimes and abuse. These measures must include “swift and effective action against hate crimes, harassment, and threats directed at individuals” and for the internet services to “keep their promises to users about their standards” (DCMS et al., 2021).
3. ‘Category 1 services’, will have to act on content that is lawful but still harmful to adults such as “abuse that falls below the threshold of a criminal offence, encouragement of self-harm and mis/disinformation.” (DCMS et al., 2021). They will also be required to protect the content of “democratic importance” and “journalistic content” (DCMS, 2021b).⁵

² Other types of harms, such as those related to intellectual property rights, data and consumer protection, and cybersecurity, were excluded from the OSB because the government has already proposed legislation to regulate them (DCMS & Home Department, 2020).

³ These definitions exclude Email, SMS and MMS, aural communication, internal business services, limited functionality services which only allow comments and reviews, as well as public bodies. (Freemont, 2021)

⁴ The absence of a clear definition of the thresholds has also received criticism. It is unclear how the duties will apply to rapidly changing companies (Freemont, 2021).

⁵ The ideas of “democratic importance” and “journalistic content” have also received criticism because of their broadness. The idea of “democratic importance” refers to content that contributes to democratic

5.2 Main policy instruments proposed in the Online Safety Bill (OSB)

Based on the approach to harmful content explained before, the OSB proposes three main policy instruments, regulatory, financial, and information-based, to fulfil the aim of “making the internet a safer place for all” (DCMS, 2021c).

Policy instruments allocate values and distribute costs and benefits (Hassel & Wegrich, n.d.) to influence behaviour of the target population. The impact assessment conducted in 2021 by the DCMS and presented to the Regulatory Policy Committee (RPC) assesses these costs and benefits by comparing possible approaches to the problem: a “do nothing” option against different ways of setting out “duties of care” towards users in the legislation. After the analysis, the option that more closely achieved “reductions in online harms while maintaining a proportionate and risk-based approach” was chosen (DCMS, 2021c).

However, as it was not its objective, the impact assessment (2021) did not analyse the main policy instruments’ appropriateness and effectiveness regarding online harms, let alone misinformation caused by political advertising in social media. Analysing how the policy instruments match the problem and institutions, provides information on whether the OSB can help to realize the broader goal of “making the internet a safer place for all” (DCMS, 2021c).

4.2.1 Regulatory instruments

Regulation sets standards of behaviour for the parties involved on a policy issue. These typically take the form of rules, bans, commands, licences and certifications (Hassel & Wegrich, n.d.). In the OSB, the behaviour standards are set based on a responsibility framework that imposes “duties of care” to providers of internet services. These duties ensure the protection of users’ wellbeing, safety and rights to freedom of expression and privacy (DCMS, 2021b) and as explained in the first part of this section, they already point to the behaviour expected of key actors.

Based on these duties, Ofcom will have to create more specific “codes of practice” for providers of internet services to assist them in complying with their obligations (DCMS, 2021b, Clauses 9 and 21). These are not only guidelines for behaviour; if necessary, they can be used as evidence in legal proceedings against non-compliant services. However, the OSB does not provide more information on how Ofcom will use them in legal settings.

Once created by Ofcom, these “codes of practice” must be sent to the Secretary of State and then to Parliament for approval (DCMS, 2021b, Clause 31.190). If Parliament disapproves, Ofcom will have to amend or reissue them. It is worth noting that despite the independence of Ofcom, the Secretary of State has the power to direct Ofcom to modify the codes of practice, especially for reasons of national security or public safety (DCMS, 2021b, Clause 33.195). Critics have deemed the closeness between Ofcom and the government as the door for potential censorship (Landi, 2021).

The “codes of practice” are but one of the bill’s mandates in a regulatory sense. Providers of internet services will also have to provide continuous risk assessments. The regulatory

political debate (DCMS, 2021a). “Journalistic content,” on the other side, refers to content generated for UK-linked journalism (DCMS, 2021a). Both types of content can appear in news publisher services.

regime as set in the OSB relies on the idea that “companies have effective systems and processes in place to understand the risk their services (including the design of those services) pose and to improve user safety” (Woods, 2021). Therefore, Ofcom will not directly monitor data from these services as a regulator. Instead, after a general risk analysis, Ofcom will require service providers to carry out risk assessments of the potentially harmful content found on their services so that they can work towards mitigation (Woods, 2021).

This provision on the draft bill offers some flexibility to regulated entities. As Hassel and Wegrich (n.d.) explain, flexibility might lead to higher levels of compliance: “when regulated entities are invited to participate in the design of regulatory standards and the control of compliance, they should also be more strongly motivated to comply.”

Nonetheless, to monitor compliance of internet services with their “duties of care,” the draft bill orders providers to publish annual “transparency reports” with the information asked by Ofcom. These will be accessible to the public for them to understand what these companies are doing to keep them safe and will be used by Ofcom to hold them accountable –also in a legal sense– whenever needed (DCMS, 2021b, Part 3. Chapter 1. Clause 49. 286)

In the specific case of misinformation and disinformation, Ofcom will create an advisory committee to clarify the scope of the regulation and provide specific advice to providers of internet services on dealing with the spread of false and inaccurate information online. The committee will include representation from users, regulated services and experts in preventing and managing online disinformation and misinformation (DCMS, 2021a. Chapter 7). The advisory committee will also be obliged to publish periodic reports accessible to the public and will have to advise Ofcom on how to use its media literacy functions to counter disinformation and misinformation (DCMS, 2021b; See also Information-based instruments in this section). However, there is no explicit mention of political advertising as a vehicle for mis/disinformation or other regulatory efforts against this phenomenon in the chapter that creates the committee. Also, it is unclear whether the committee’s advice will later be part of the “codes of practice” or of the risk assessment, and how Ofcom will assess internet services’ compliance with regards to mis/disinformation.

Finally, as an enforcement method, the draft bill also provides “liability of corporate officers” of internet services’ who continuously fail to fulfil their duties, although with no clear rules for how this might apply. These measures will be taken in cases of continuous non-compliance. They are the ‘last resort’ to be used by the government and can be challenged in the justice system (Woods, 2021). As stated in the FGR, there is a risk that including this provision in the regulation will have a higher effect on smaller companies and investment (DCMS & Home Department, 2020; Freemont, 2021).

4.2.2 Financial incentives

Regulatory instruments rarely work on their own to change the behaviour of the target population. Whenever they are not enough or an extra push is needed, financial incentives are beneficial (Hassel & Wegrich, n.d.). While positive incentives such as subsidies can encourage a behaviour, negative incentives such as fines and business disrupting mechanisms can deter undesirable behaviour as they act as a financial punishment for non-compliance to the law.

The OSB also relies on financial disincentives to enforce the regulation of harmful content online. It makes provision for Ofcom to impose penalties “appropriate” and “proportionate to the failures” of services providers (DCMS, 2021a). The maximum amount for such penalties is £18 million or 10% of worldwide revenue (DCMS, 2021a. Clause 85). These maximum penalties are very high, even compared to other similar legislation: for example, the DSA currently discussed in the European Commission sets fines up to 6% global turnover (Dickson & Goujard, 2021). The idea behind such an amount is to prevent service providers from ignoring the regulation and guarantee their compliance with the authorities.

The OSB also considers business disruption measures, another disincentive affecting providers’ revenue. Ofcom will require providers to withdraw access to certain services or to entirely block them in the UK for severe non-compliance. These provisions must be proportional to the offense as well as pass through court, and Ofcom must immediately inform the Secretary of State about them (DCMS, 2021a. Clause 94-95; Woods, 2021).

However, not many details are included on the bill to clarify when Ofcom will use these incentives against providers, other than the idea that the continued failure to comply with the duties stated in the OSB will have consequences. The OSB explains that when this continued behaviour is detected, Ofcom must issue a confirmatory decision and a notice of the penalty (DCMS, 2021a. Clause 86). However, the draft is still unclear about how to measure continued infractions, when each penalty will be incurred, and how to calculate the revenues.

4.2.3 Information-based instruments

Information-based instruments work by “disseminating various forms of information to target populations in order to encourage or discourage certain behaviours” (Hassel & Wegrich, n.d.). Product labelling, such as misinformation flags in social media, and the restriction of information in advertising are two well-known information-based instruments.

These instruments are not clearly outlined in the draft bill but appear under the need to improve the UK’s media literacy. The OSB aims to expand Ofcom’s existing duties related to media literacy to include digital media literacy. As the primary regulator, Ofcom can “encourage regulated service providers and broadcasters to use and develop tools” including “technologies and systems which help users to identify what type of material they are seeing (for example, sponsored content), how reliable and accurate content it is, and how users can control the material they receive.” (DCMS, 2021b).

Although the OSB has no explicit provisions regarding labelling of online content, Ofcom can ask providers of internet services to do so if it allows for the improvement of digital media literacy. This fact provides an opportunity to assess misinformation and disinformation through labelling and other information-based mechanisms. Since the Advisory Committee on Misinformation and Disinformation (also referred to as “advisory committee” before) will advise Ofcom regarding the best ways to enhance recognition of false and misleading communications online, these instruments might be useful (DCMS, 2021a).

Furthermore, the role of Ofcom regarding media literacy can also open the door for the identification or flagging of paid political advertising, a known vehicle against misinformation. Labelling misinformation in ads can be mandated similarly to the digital imprint for political ads proposed in the Election Bill (The Electoral Commission, 2021). Despite the difference in scopes of both bills, coordination and communication between regulators can prevent repeated work and increase the efficiency and enforceability of the overall UK regulatory regime of internet services (Woods, 2021).

Other types of information-based instruments include strategies and campaigns aimed at building user capacities. The OSB also calls for long-term strategies such as public awareness campaigns and training to improve teachers' skills. No explicit provision on how to implement this strategy is provided in the draft bill, but the DCMS launched a Digital Media Literacy Strategy earlier this year with more specific guidelines for schools, libraries, and support for educational institutions. The strategy has a more stringent focus against misinformation and disinformation by strengthening information literacy, critical thinking skills and understanding of the journalistic process.

However, educators have criticised it for not conjoining the efforts of Ofcom as the regulator of internet services and the provider for media literacy. In their views, regulation and media literacy are still two different strategies in which the weight of responsibility of spotting misinformation is assigned to users and not to the services it is supposed to regulate. A cause of this difference is that the media literacy strategy is not so clearly outlined in the draft bill and doesn't appear to be a primary objective of the legislation (Livingstone, 2021). This critique points to the capacity of Ofcom to implement a two-sided policy with equal standards, which is something that must be also discussed in upcoming stages of the policy process.

5.3 Potential unintended effects of the OSB: a free pass to political advertising?

As discussed before, the policy instruments used in the OSB are based on a responsibility framework that leaves some room for providers of internet services to act on the risks posed by their services and report back on their findings to Ofcom. Despite this involvement might lead to higher levels of compliance, as suggested by Hassel and Wegrich (n.d.), some problems might affect Ofcom's capacity to regulate internet services.

The first one is related to the time necessary to create a common ground and the specific codes of practice, without counting the time for the bill to become law. Although the regulation of harmful content and misinformation is urgent, setting the risk assessments, transparency standards, and advisory committee's advice will need at least a year to be completed. The road to approving the codes of practice can likewise end on a back-and-forth dynamic in Parliament, which might make the process too slow. It might also give a free pass to providers of internet services because the codes might be too general or obsolete to enforce.

The second concern is transparency. Although providers are required to use their knowledge on their infrastructure, they might not have incentives to disclose information that spreads harmful content on the online sphere: in the case of Category 1 services, such content is related to the recommendation algorithms, payment for ads, users who have a preferential treatment because of their followers, among others. Therefore, there is a

chance that the OSB will only be forcing Category 1 services to comply with their terms of service (Woods, 2021). If that is the case, the regulatory framework proposed in the OSB can end up being only a different, more complicated way of letting providers self-regulate their services.

Third, and related explicitly to political advertising: Although the Advisory Committee on Misinformation and Disinformation will be able to more precisely define the contents and practices to be banned or regulated, the OSB's neglect to mention of political advertising as a vehicle for mis/disinformation could have the unintended consequence of giving it a "free pass." Although there are other efforts to imprint digital political ads, the lack of coordination and collaboration between regulators can either double efforts or completely ignore the problem. In this sense, details on the risks of misinformation through political advertising, such as manipulating voters through micro-targeting, deepfakes and disinformation campaigns (The Constitution Unit, 2021), must be considered in both cases settings to define transparent workflows to adequately address them.

6 Weaknesses, loopholes, ambiguities

Given the OSB's current legislative stage, it should be stated that all mentioned weaknesses are theoretically still subject to change. Therefore, all points that are going to be made in this section refer to the version of the bill, which is currently scrutinised by the joint pre-legislative committee. As the OSB is a multi-dimensional legislative effort to tackle multi-facetted problems, there are multiple weaknesses and blind spots to highlight regarding political advertisement and political misinformation.

Firstly, one of the more fundamental questions regarding the OSB is the definition of what "harmful but legal" content is. The bill remains vague on how to distinct between content that is "harmful but legal" and "justiciable." The lack of clarity poses a challenge for all involved stakeholders, from Ofcom to the providers of internet services. Ambiguity on Ofcom's side could lead to a lack of enforcement and confusion for providers. This could end in lack of follow-through with their "duty of care." It seems as if lawmakers were so ambitious with what they were trying to achieve with this bill, that they failed to deliver an enforceable legislative proposal.

The draft bill is mainly focussed on protecting individuals from online harm but does not acknowledge the danger of online harms for democratic institutions, the political climate as well as democracy itself. Recent events have shown that the harms arising on social-media platforms often relate to societal issues more so than individual well-being. Misinformation on COVID-19 vaccines, climate change or migration are difficult to trace as well as measure their potential impact. Tech companies have shown to be either incapable or unwilling to regulate this type of content as their algorithms in large part help with circulating it and to an extent form the basis for their business models. As private companies, they ultimately do not serve public interest like public institutions would. While the long-term effect of political misinformation is yet to be examined, not addressing it entirely in the OSB could cause serious harms to political discourse as well as deterioration of trust in political institutions.

As currently constructed, the OSB has no standardised conditions for providers of internet services on how to deal with political advertising. Today, these companies have differing policies in place which are subject to frequent changes and not aimed towards the specific needs of the UK's democratic system. This forms an inconsistent and unpredictable framework, which makes the evaluation of advertising content difficult. As previously mentioned, none of the tech companies with their policies in place have been successful with regulating such content and harmonising different policies will become increasingly difficult once the OSB has been passed, as legislative processes in the UK have shown to be lengthy procedures that have difficulties adapting to the pace of disruptive changes happening on the internet.

Furthermore, tech companies still being allowed to carry out their individual policies for removing political advertising could end up in a censorship of legitimate and legal political advertising.

While the draft aims to act against user-generated fraud and scams, it fails to include measures against misinformation campaigns organised through advertising or fake websites. The bill neglects the danger resulting from organised advertising efforts, for example in the run-up to elections, which can shift political developments. The tech companies' tools for users to create targeted ads are open to anyone willing to pay for them. As paid-for advertising and promoted posts make up for a large part of the business model for these companies, it remains to be seen whether they actually have incentives to fight this type of content.

In its current form the draft bill details two specific duties in addition to the previously mentioned "duty of care." The bill is very specific in outlining the duty for providers of internet services to protect journalists' freedom of expression while subjecting other citizens to terms that could potentially harm theirs. Secondly, the bill mentions the duty of these providers to protect content of "political importance" that contributes to political developments in the UK.

In many cases, protecting journalistic freedom is desirable, but when it comes to political misinformation, the view posed in the bill could be a bit more nuanced. Past years have shown that authoritarian states have increasingly used government-affiliated news outlets to spread inaccurate news and destabilise democratic institutions in foreign countries. Furthermore, the UK has already witnessed the effects of prominent journalists spreading inaccurate information live on-air, which happened without contextualisation or challenge by authorities. The legislative text if adopted could not only be a licence for journalistic exploitation but could, in the long-run, harm peoples' trust in reputable news sources as well as undermine credibility of democratic institutions.

Technical developments have made it possible for political actors to specifically target individuals over the internet based on the analysis of digital personal data. This type of "micro-targeting" of potential voters has taken place during the Brexit referendum and has the potential of negatively influencing free voting. The bill, as currently proposed, has no proposed measurements on how to either protect personal user data or to limit targeting of individuals.

In general, all outlined legislative measures against online harms put an administrative burden on Ofcom. The institution will be tasked with enforcing the outlined laws, but it will also have to regularly redefine what “harmful but legal” content is, as content circulated on social media constantly changes. Additionally, they will be required to outline a long-term strategy on how to deal with the increasing misinformation and disinformation published on the internet. It remains to be seen, whether Ofcom has the administrative and human capacity to follow-through on the mentioned tasks.

7. Recommendations

1. Avoid legal ambiguity by providing clear definitions on what “harmful content” is

To make this bill a success from the beginning the idea of “harmful content,” especially the “harmful but legal” content must be clearly defined. A law based on a vague concept has little chance of being effective. A proper definition would limit the scope of the bill to avoid future problems. Additionally, too much freedom of censorship for tech companies could endanger hard fought democratic rights. A blueprint for this could be the Digital Services Act which is currently being evaluated by the EU and is rather clear on what type of content will be subject of regulation.

2. Common approach to identifying political advertising and other advertising

The UK government should develop a consistent framework in which tech companies, not the government, are able to recognise and classify political advertising content. The framework could involve multiple stages and steps, which end in the classification of “political” and “non-political” content. The “digital imprint” proposed in the Election Bill might be the first step towards such an effort, but it needs to be well defined and harmonised with other provisions on misinformation and disinformation, as subject to the OSB.

3. Country-wide standards for political advertising online

Disclosing all required information and context to understand each published piece could be made a requirement for tech companies publishing content online. This information could include publisher, publisher background, political affiliation, underlying algorithm and whether the algorithm targets a specific audience. There is also a need for a harmonisation between the regulation of political advertising online and offline. It should not make a difference whether misinformation is spread on broadcasting platforms like newspaper and the TV or the internet.

4. Address collective harm and mistrust in institutions in the OSB

As previously outlined, the OSB fails to deliver on collective harms. It is fair to say that sometimes it is not easy to distinguish between individual and collective harm, as the former can become the latter in some cases. But as recent leaks and whistle-blowers have revealed, tech companies such as Facebook make money from circulating harmful content. The OSB should make provisions to limit such activities.

5. Reframe the risks of political advertising as “deteriorating trust in political parties and the UK democracy”

Currently in the UK, mis/disinformation in political advertising is not receiving the attention it needs. Despite evidence of its dangers, it can get a “free pass” in the current discussions, because there is little incentive in the political sphere to regulate it. Furthermore, misinformation spread through political advertising currently lies between two regulatory proposals (the OSB, which targets harms to individuals, and the Election Bill, which aims to regulate political advertising as such) with little clarity on the scope of each respective bill in addressing misinformation in political advertising online.

Reframing political advertising as “deteriorating trust in political parties and the UK democracy,” can persuade more political actors of the importance of issuing a strong regulation on this issue. This has already begun with civil society actors pointing to the dangers of deepfakes, bots and fake accounts that “confuse the information environment” and undermine trust in the institutions (Constitution Unit, 2021). However, a strong process of agenda setting is needed in this case on the part of independent regulators, the media, civil society and the private sector so that online political advertising is no longer viewed by political actors as a legitimate way to obtain votes and political power, but rather a risk to their credibility and to UK democracy.

6. Define content / tasks for providers of internet services in the codes of practice and involve public institutions

As currently constructed, the bill gives most of the responsibility for regulation to tech companies as part of their “duty of care.” These providers will have to then produce their codes of practices, which will then be verified and enforced by Ofcom. However, given that their current practices are rooted in their business models, it is fair to remain sceptical whether this will be the most effective measure against political mis/disinformation.

More specific common principles against these issues need to be directly determined in the draft OSB, as well as specific responsibilities concerning content moderation, algorithmic fairness and flagging of political advertisement. Ofcom as well as the Electoral Commission should include the forthcoming recommendations of the Mis/disinformation Committee in the codes of practice for each platform provider, including what justiciable content is and how to handle misinformation and disinformation.

7. Involve public institutions

One way to ensure that public interest is being served is to guarantee that providers are accountable to the greater public. Involving public institutions with clear responsibilities and powers can be a good way to do this, as they can be the contact with the public (for example, through ombudspersons or someone to go to in case of complaints), the regulators and the government. This would also require some joint work with the Electoral Commission, the regulator of political finance and elections in the UK, to better determine clear and concise rules to flag political advertisement and misinformation online. This could look like a model of collective responsibility, shared by public institutions, platform providers, and government.

8. Assess and strengthen the capacity of Ofcom

No regulation can work without a capable regulator. Although Ofcom already does a good job regulating media and promoting data literacy in the UK, the jump to the regulation of social media is considerable. The OSB must better clarify the scope of Ofcom’s

responsibilities, how they overlap and how they connect to one another and to the role of other regulators of digital technologies, such as Competition and Markets Authority and Information Commissioner's Office in the case of privacy and digital markets (Woods, 2021).

Particularly, the OSB should prevent the politicisation of Ofcom by making it an independent organisation like the Bank of England. Staff at Ofcom should be restricted in participating in political roles and selection of employees should be based on expertise. To safeguard the independence of Ofcom and prevent the disclosure of insider information, OSB should require the creation of an ethics framework. Also, the UK government must make sure that Ofcom has the right funding and infrastructure to fulfil its task.

9. Encourage algorithm transparency and promote fact-checked content to limit misinformation

Platform algorithms in their current version cause harm to democracy and collective well-being and serve as circulators for problematic content instead of limiting it. Transparency must be the standard to evaluate algorithms so that the public can take more informed decisions regarding their health and wellbeing. Furthermore, reprogramming the algorithms could help to limit the reach of political misinformation as well as targeted advertising. Ending the current promotion of such content could reduce the harms resulting from it. The promotional efforts in the algorithms could instead focus on fact-checked content from official sources and institutions which would benefit the overall health of society.

10. Instalment of democracy hub

Once algorithms would start promoting fact-checked information, this could be the first step towards a central information hub which collects and presents information and news from trustworthy and reliable sources. It should be ensured that this hub would present well-balanced information and could be run by an independent, yet to be founded, institution. An exemplary website is the "BBC News Reality Check," which could serve as a model for this hub.

8. Conclusion

The lack of regulation of online political advertising and mis/disinformation is still an overlooked problem in the UK. As the analysis presented in this paper shows, despite the UK being in the middle of the discussion of the OSB, this phenomenon is not entirely recognised nor regulated. Although it is part of the online harms that the bill is supposed to address, its approach is very vague and doesn't provide clear guidelines on how to tackle it. Furthermore, there is little willingness to do so on the part of political actors and there is no clarity as to the capacity of Ofcom, the designated regulator, to enforce the OSB.

Based on these insights, this paper offers ten recommendations. They highlight the necessity of avoiding ambiguity in the wording of the bill, guaranteeing the independence of Ofcom as a regulator and reframing the bill so that it recognises collective harm and the danger that political mis/disinformation can cause to democracy in the UK. These

recommendations have the potential to significantly increase the impact of the current proposal and allow it to tackle the dangers of political mis/disinformation to UK democracy.

References

- Ackermann, F. and Eden, C. (2011). Strategic Management of Stakeholders: Theory and Practice. Long Range Planning, 44: 179-96.
- Advertising Standard Authority (2020, 3 June). We think political advertising should be regulated. ASA, <https://www.asa.org.uk/news/we-think-political-advertising-should-be-regulated.html> [Accessed 14.12.2021]
- Advertising Standard Authority (2021, 15 April). Why we don't regulate political ads. ASA, <https://www.asa.org.uk/news/why-we-don-t-regulate-political-ads.html> [Accessed 14.12.2021]
- Advertising Standard Authority (n.a.). 07 Political and controversial matters. ASA, https://www.asa.org.uk/type/broadcast/code_section/07.html [Accessed 14.12.2021]
- Advertising Standard Authority (n.a.). What we cover. ASA, Auspex Internationa (n.a.). What we believe in. <https://www.auspex.ai/what-we-believe> [Accessed 14.12.2021]
- Allington, D., Duffy, B., Wessely, S., Dhavan, N., & Rubin, J. (2021). Health-protective behaviour, social media usage and conspiracy belief during the COVID-19 public health emergency. Psychological Medicine, 51(10), 1763–1769. <https://doi.org/10.1017/S003329172000224X>
- Barton, M., Duncan, P., McIntyre, N., Pegg, D. and Smith, J. (2019, 19 November). UK election: which parties are winning the online war for ads, cash and votes? The Guardian, <https://www.theguardian.com/politics/2019/nov/12/uk-election-parties-winning-online-war-ads-cash-votes-digital-dashboard> [Accessed 14.12.2021]
- BBC News (2021, 19 November). Nadine Dorries: Culture secretary says social media has been hijacked. BBC News, <https://www.bbc.com/news/entertainment-arts-59305080> [Accessed 14.12.2021]
- BBC RealityCheck (n.a.) Reality Check. https://www.bbc.com/news/reality_check [Accessed 14.12.2021]
- Brennen, J. S., Simon, F. M., Howard, P. N., & Nielsen, R. K. (n.d.). Types, Sources, and Claims of COVID-19 Misinformation. 13.
- Brändle, V. K., Galpin, C., & Trenz, H.-J. (2021). Brexit as 'politics of division': Social media campaigning after the referendum. Social Movement Studies, 1–20. <https://doi.org/10.1080/14742837.2021.1928484>
- Cabinet Office. (2020). Transparency in digital campaigning: technical consultation on digital imprints. London.
- Constitution Unit (2020, 10 July). Digital technology and the resurrection of trust: the report of the House of Lords Democracy and Digital Technologies Committee. The Constitution Unit Blog, <https://constitution-unit.com/2020/07/10/digital-technology-and-the-resurrection-of-trust-the-report-of-the-house-of-lords-democracy-and-digital-technologies-committee/> [Accessed 14.12.2021]
- DCMS, and Home Department. (2020, December 15). Online Harms White Paper: Full government response to the consultation – GOV.UK. Gov.Uk. <https://www.gov.uk/government/consultations/online-harms-white-paper/outcome/online-harms-white-paper-full-government-response#part-2-what-harmful-content-or-activity-will-the-new-regulatory-framework-apply-to-and-what-action-will-companies-need-to-take> [Accessed 08.12.2021]
- DCMS, Home Office, and Dowden, O. (MP). (2021, May 14). Landmark laws to keep children safe, stop racial hate and protect democracy online published – GOV.UK. Gov.Uk. <https://www.gov.uk/government/news/landmark-laws-to-keep-children-safe-stop-racial-hate-and-protect-democracy-online-published> [Accessed 28.11.2021]
- DCMS. (2021a). Draft Online Safety Bill. Gov.Uk, 145. <https://www.gov.uk/government/publications/draft-online-safety-bill> [Accessed 28.11.2021]
- DCMS. (2019). Online Harms White Paper. <https://www.gov.uk/government/consultations/online-harms-white-paper/online-harms-white-paper>
- DCMS. (2021b). Online Safety Bill: Explanatory Notes. Gov.Uk. <https://www.gov.uk/government/publications/draft-online-safety-bill> [Accessed 28.11.2021]
- DCMS. (2021c). Title: The Online Safety Bill Summary: Intervention and Options RPC Opinion: Informal review 1 Summary: Analysis and Evidence Policy Option 1 Description: A duty of care for user generated content and activity addressing illegal harms and safeguarding child. In gov.uk.
- Dickson, A. (2021, 21 November). UK's top digital minister vows 'tougher and stronger' Online Safety Bill. Politico.eu, <https://www.politico.eu/article/nadine-dorries-online-safety-bill-uk/> [Accessed 14.12.2021]
- Dickson, A., and Goujard, C. (2021, November 8). On online content, London tries to out-regulate Brussels – POLITICO. Politico. <https://www.politico.eu/article/eu-digital-services-act-uk-online-safety-bill-content-moderation-safety/> [Accessed 28.11.2021]
- Edwards, L. (2021). Can the Online Safety Bill be more than a toothless tiger (or a Facebook flop), <https://blogs.lse.ac.uk/mediase/2021/10/11/can-the-online-safety-bill-be-more-than-a-toothless-tiger-or-a-facebook-flop/> [Accessed 10.12.2021]
- Electoral Commission (2019). UK Parliamentary General Election 2019. The Electoral Commission, <https://www.electoralcommission.org.uk/sites/default/files/2020-04/UKPGE%20election%20report%202020.pdf> [Accessed 14.12.2021]

- Electoral Commission (2021, 11 March). Claims made in online political ads. The Electoral Commission, <https://www.electoralcommission.org.uk/i-am-a/voter/online-campaigning/claims-made-online-political-ads> [Accessed 14.12.2021]
- Electoral Commission (n.a.). Who we are. The Electoral Commission, <https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/who-we-are> [Accessed 14.12.2021]
- Facebook (n.a.). Facebook-Werbebericht. <https://www.facebook.com/ads/library/report/?source=archive-landing-page&country=GB> [Accessed 14.12.2021]
- Financial Conduct Authority (2016). Protecting Consumers. <https://www.fca.org.uk/about/protecting-consumers> [Accessed 14.12.2021]
- Financial Conduct Authority (2020). Perimeter Report. <https://www.fca.org.uk/publication/annual-reports/perimeter-report-2020-21.pdf> [Accessed 14.12.2021]
- First Draft (2019, 14 November). UK Election: How political parties are targeting voters on Facebook, Google and Snapchat ads. First Draft, <https://firstdraftnews.org/articles/uk-election-how-political-parties-are-targeting-voters-on-facebook-google-and-snapchat-ads/> [Accessed 14.12.2021]
- First Draft (n.a.). About. First Draft, <https://firstdraftnews.org/about/> [Accessed 14.12.2021]
- Freemont, L. (2021, May 13). The Online Safety Bill, what is in it and what does it mean for techUK members. TechUK. <https://www.techuk.org/resource/the-online-safety-bill-what-is-in-it-and-what-does-it-mean-for-techuk-members.html> [Accessed 03.12.2021]
- Galston, W., Political Knowledge, Political Engagement, and Civic Education, Annual Review of Political Science 2001 4:1, 217-234)
- Google (n.a.). Publicité à caractère politique au Royaume-Uni. <https://transparencyreport.google.com/political-ads/region/GB> [Accessed 14.12.2021]
- GOV.UK (2019a, 8 April). Consultation outcome – Online Harms Paper. GOV.UK, <https://www.gov.uk/government/consultations/online-harms-white-paper> [Accessed 14.12.2021]
- GOV.UK (2021, 10 March). The Digital Regulation Cooperation Forum. GOV.UK, <https://www.gov.uk/government/collections/the-digital-regulation-cooperation-forum> [Accessed 14.12.2021]
- Harbinja, E., The UK's Online Safety Bill: Safe, Harmful, Unworkable?, <https://verfassungsblog.de/uk-osb/> [Accessed 17.12.2021]
- Hassel, A., and Wegrich, K. (n.d.). How to do Public Policy. Forthcoming.
- House of Commons Library. (2019). Who regulates political advertising? London.
- House of Lords (2019). Digital Technology and the Resurrection of Trust. Authority of the House of Lords, <https://committees.parliament.uk/publications/1634/documents/17731/default/> [Accessed 14.12.2021]
- Information Commissioner's Office (n.a.). Home Page. <https://ico.org.uk/> [Accessed 14.12.2021]
- Jerit, J., and Zhao, Y., Political misinformation in: Annual Review of Political Science, 2020, p.77-94)
- Labour Party (2019). Digital Campaigning Guide. The Labour Party, https://labour.org.uk/wp-content/uploads/2019/11/PRINT-READY-12671_19-Digital-Guide-2019-v3-IN-HOUSE.pdf [Accessed 14.12.2021]
- Labour Party (2019). It's time for real change. The Labour Party Manifesto 2019, <https://labour.org.uk/wp-content/uploads/2019/11/Real-Change-Labour-Manifesto-2019.pdf> [Accessed 10.05.2022]
- Landi, M. (2021, May 13). Online Safety Bill labelled 'state-backed censorship' by campaigners | Evening Standard. Evening Standard. <https://www.standard.co.uk/news/uk/safety-ofcom-oliver-dowden-government-prime-minister-b934893.html> [Accessed 28.11.2021]
- Lee, G. (2021), Why the Online Safety Bill fails, and what can make the Internet safer, <https://www.pharmaceutical-technology.com/features/why-the-online-safety-bill-fails-and-what-can-make-the-internet-safer/> [Accessed 11.12.2021]
- Lords Committee on Democracy and Digital Technologies. (2020, June 29). Democracy under threat from 'pandemic of misinformation' online, say Lords Committee – Committees – UK Parliament.' UK Parliament. <https://committees.parliament.uk/committee/407/democracy-and-digital-technologies-committee/news/115316/democracy-under-threat-from-pandemic-of-misinformation-online-say-lords-committee/> [Accessed 20.11.2021]
- Mair, J., Clark, T., Snoddy, R., & Tait, R. (Eds.). (2017). Brexit, Trump and the media. Abrams academic publishing.
- Marshall, H., & Drieschova, A. (2018). Post-Truth Politics in the UK's Brexit Referendum. New Perspectives, 26(3), 89–105. <https://doi.org/10.1177/2336825X1802600305>
- Ofcom a. (2021). Ofcom Coronavirus Survey https://www.ofcom.org.uk/_data/assets/excel_doc/0020/25083/ofcom-coronavirus-data-tables-week76-sep.xlsx [Accessed 20.02.2022]
- Ofcom b. (2021). News Consumption in the United Kingdom (UK) 2021. https://www.ofcom.org.uk/_data/assets/powerpoint_doc/026/222479/news-consumption-in-the-uk-2021-report.ppt [Accessed 20.02.2022]

- Ofcom c. (2021). What is Ofcom? Ofcom.Org. <https://www.ofcom.org.uk/about-ofcom/what-is-ofcom> [Accessed 14.12.2021]
- Office of Communication (2020). London Real: COVID-19. Ofcom Broadcast and OnDemand Bulletin, https://www.ofcom.org.uk/_data/assets/pdf_file/0020/194402/sanction-decision-estv.pdf [Accessed 14.12.2021]
- Office of Communication (2021, 4 February). Insights for online regulation: A case study monitoring political advertising. Ofcom Economics discussion paper series, 3, https://www.ofcom.org.uk/_data/assets/pdf_file/0020/212861/tools-for-online-regulation.pdf [Accessed 14.12.2021]
- Parliament of the United Kingdom. (2003). Communications Act. London.
- Parliamentlive.tv (2021, 18 October). Draft Online Safety Bill (Joint Committee). Parliamentlive.tv, <https://www.parliamentlive.tv/Event/Index/348d8do4-3876-4220-a4of-906f210686fe> [Accessed 14.12.2021]
- Reeves, P. (2013). Local political marketing in the context of the conservative party. Journal of Non-Profit and Public Sector Marketing, https://usir.salford.ac.uk/id/eprint/33659/3/JOURNAL_OF_NON-PROFIT_AND_PUBLIC_SECTOR_MARKETING_SUBMISSION.pdf [Accessed 14.12.2021]
- Schraer, R. (2019, 14 November). General election 2019: Are Lib Dem bar charts and posts on tactical voting misleading people? BBC News, <https://www.bbc.com/news/uk-politics-50375532> [Accessed 14.12.2021]
- Snap (n.a.). Snap Political Ads library. <https://snap.com/en-GB/political-ads> [Accessed 14.12.2021]
- Stone, J. and Woodcock, A. (2021, 19 November). Boris Johnson slaps down Nadine Dorries over freedom of speech online. Independent, <https://www.independent.co.uk/news/uk/politics/nadine-dorries-culture-secretary-social-media-b1960665.html> [Accessed 14.12.2021]
- Tambini, D. (2021, 6 August). The Online Safety Bill is being opposed on “free speech” grounds—but we urgently need protection from platforms. Prospect Magazine, <https://www.prospectmagazine.co.uk/politics/online-safety-bill-social-media-platforms-government-parliament> [Accessed 14.12.2021]
- The Constitution Unit. (2021, April 13). Online harms to democracy: the government’s change of approach | The Constitution Unit Blog. The Constitution Unit Blog. <https://constitution-unit.com/2021/04/13/online-harms-to-democracy-the-governments-change-of-approach/> [Accessed 28.11.2021]
- The Electoral Commission. (2018). Report: Digital campaigning - increasing transparency for voters. London.
- The Electoral Commission. (2021, July 5). Introducing digital imprints | Electoral Commission. Electoral Commission Online. <https://www.electoralcommission.org.uk/who-we-are-and-what-we-do/our-views-and-research/elections-bill/introducing-digital-imprints> [Accessed 15.12.2021]
- Tidy, J. and Schraer, R. (2019, 17 December). General election 2019: Ads are 'indecent, dishonest and untruthful'. BBC News, <https://www.bbc.com/news/technology-50726500> [Accessed 14.12.2021]
- Turcilo, L., and Obrenovic, M. (2020), Misinformation, Disinformation, Malinformation: Causes, Trends, and Their Influence on Democracy, https://www.boell.de/sites/default/files/2020-08/200825_E-Paper3_ENG.pdf [accessed 15.12.2021]
- Twitter (n.a.). Ads transparency. <https://business.twitter.com/en/help/ads-policies/product-policies/ads-transparency.html> [Accessed 14.12.2021]
- UK Finance (2021, 12 May). UK Finance responds to the Government's draft Online Safety Bill. <https://www.ukfinance.org.uk/press/press-releases/uk-finance-responds-governments-draft-online-safety-bill> [Accessed 14.12.2021]
- UK Parliament (2021). No longer the land of the lawless: Joint Committee reports. UK Parliament, <https://committees.parliament.uk/committee/534/draft-online-safety-bill-joint-committee/news/159784/no-longer-the-land-of-the-lawless-joint-committee-reports/> [Accessed 14.12.2021]
- UK Parliament (n.d.). Coalition for Reform in Political Advertising – written evidence (DAD0092). UK Parliament, <https://committees.parliament.uk/writtenevidence/590/pdf/> [Accessed 14.12.2021]
- UK Parliament (n.d.). Committees – Draft Online Safety Bill (Joint Committee). UK Parliament, <https://committees.parliament.uk/committee/534/draft-online-safety-bill-joint-committee/news/> [Accessed 14.12.2021]
- UK Parliament (n.d.). Democracy and Digital Technologies Committee – role. UK Parliament, <https://committees.parliament.uk/committee/407/democracy-and-digital-technologies-committee/role/> [Accessed 14.12.2021]
- UK Parliament (n.d.). MPs and Lords – Damian Collins. UK Parliament, <https://members.parliament.uk/parties/Commons> [Accessed 14.12.2021]
- UK Parliament (n.d.). MPs and Lords – State of the parties. UK Parliament, <https://members.parliament.uk/member/3986/contact> [Accessed 14.12.2021]
- UK Parliament (n.d.). What is a draft bill? UK Parliament, <https://www.parliament.uk/about/how/laws/draft/> [Accessed 14.12.2021]
- UK Parliament (n.d.). Written evidence submitted by Twitter. UK Parliament, <https://committees.parliament.uk/writtenevidence/39199/pdf/> [Accessed 14.12.2021]

UK Statistics Authority (n.a.). What we do. <https://uksa.statisticsauthority.gov.uk/what-we-do/> [Accessed 14.12.2021]

Wakefield, J. (2021, 6 December). Online Safety Bill: What to expect. BBC News, <https://www.bbc.com/news/technology-59509702> [Accessed 14.12.2021]

Wardle, C., (2019), Misinformation has created a new world order in: Scientific American
Whogets.me (2021, 3 September). Why (and how) the UK Online Safety Bill should regulate political ads. <https://whotargets.me/en/online-safety-and-political-advertising/> [Accessed 14.12.2021]

Whogets.me (n.a.). About. <https://whotargets.me/en/about/> [Accessed 14.12.2021]

Wikipedia (2021). Damian Collins, Wikipedia, https://en.wikipedia.org/wiki/Damian_Collins [Accessed 14.12.2021]

Woods, L. (2021). The UK 's Approach to Regulation of Digital Platforms. In J. Bayer, B. Holznapel, P. Korpisaari, and L. Woods (Eds.), Perspectives on Platform Regulation. Concepts and Models of Social Media Governance Across the Globe (1st. Editi, pp. 329–350). Nomos.

This publication reflects only the personal views of the authors. Publication under Creative Commons license CC BY-ND. Reprinting and other distribution – including excerpts – permitted only with acknowledgment of source • original version © Centre for Digital Governance – Hertie School, Berlin 2022

Friedrichstraße 194
D – 10117 Berlin
Tel.: +49 (0)30 259219-0

Online: hertie-school.org/centre-for-digital-governance/
E-Mail: info@hertie-school.org
Twitter: @thehertieschool