

Written Evidence submitted by Index on censorship (OSB06)

Public Bill Committee on the Online Safety Bill

Executive Summary

The Online Safety Bill has simple, laudable aims - to make the online sphere more safe. But despite almost seven years of debate, thousands of hours of Parliamentary scrutiny, analysis from civil society, business and the media, there is still significant uncertainty about how the Bill will work in practice. The Government is still not able to define terms at the heart of the legislation such as “legal but harmful” or give the as many as 180,000 technology companies big and small who will implement this new legal framework clear guidance on how this landmark legislation should operate.

To fill this gap and help explain what the Bill will mean in practice, the Legal to Say Legal to Type campaign has instructed media law expert Gavin Millar QC of Matrix Chambers to produce **the first analysis of the implications of the Online Safety Bill on UK citizens’ freedom of speech** (‘the Legal Opinion’).

The QC’s opinion explains and analyses the broad implications of the Government’s new online safety regime against current freedom of expression laws and found that the Bill will significantly curtail freedom of expression in a way that has profound consequences for the British media and journalism, courts and the UK’s digital economy. The Bill gives the Secretary of State overseeing the legislation unprecedented powers to curtail freedom of expression with limited parliamentary scrutiny.

The Bill, which received a second reading in Parliament on 19 April, does not comply with Article 10 of the European Convention on Human Rights, and far from the claim of the Culture Secretary that the Bill will protect free speech it actively undermines existing legal protections in an unprecedented manner. **This new analysis shows how the Online Safety Bill as currently drafted ends the historic principle in law that people can publish what they like, unless the state specifically and clearly passes laws to the contrary.**

This report is not a comprehensive dissection of the flaws in the Bill which are too vast to deal with succinctly. For example, the UK Independent Reviewer of Terrorism Legislation, Jonathan Hall QC has recently publically criticised the Bill as being ‘*ineffective on terrorism*’. The chief criticism he lays is that “*the Bill defines "terrorism content" by reference to*

terrorism legislation, but ignores intention and defences. This leads to some very odd outcomes. It's hard to see how it provides a workable framework for regulation."

The ambiguity of the drafting and the lack of governmental consideration on the Bill's intersection with existing linked areas of law is indeed staggering. The idea that speech can be lawfully moderated without properly adjudicating on an individual's intention and the context of the speech is nonsensical - irrespective of whether your concern is terrorism, crime or freedom of expression.

Index on Censorship believes that the consequences of the Bill (intended and unintended) go beyond what has been considered in Parliament to date, for example:

- **The Bill violates freedom of speech as defined in UK and international law.** The government has failed to take onboard previous recommendations by the Joint Committee on the draft Bill for better protections for freedom of expression, and to comply with Article 10 of the ECHR. The wide-reaching 'Duty of Care' with its precautionary principle, a concept lifted from health and safety legislation, is not applicable to online speech. In the Bill, the duty to censor content with a 'material risk of significant harm to an appreciable number of adults', means that platforms will need to assess not whether content is illegal or not, before restricting access, but will have a duty to proactively censor content with the *potential* to cause harm. This will disproportionately impact the voices of marginalised people.
- **Protections for media content are not as wide as existing human rights for journalists** because the Online Safety Bill does not mandate protection in principle for all journalism (or even all journalism of public interest value). Only content that is 'likely to be of interest to a significant number of UK users' and that is 'reasonably considered to be UK-linked journalism' is protected. This means that content from the New York Times, Mail Online US or Guardian US, among many others, could be censored arbitrarily and be removed from social media platforms before appeals are lodged by publishers. The Bill only protects published journalism, not the practice of journalism, and by enforcing algorithmic censorship in the UK it may become harder for UK journalists to report on complex world events or undertake investigative journalism.
- **Pro-active state-enforced censorship by algorithm has questionable legality.** The legal opinion demonstrates how censorship by algorithm is likely to be

challengeable in the courts as it is a legal requirement for restrictions on free speech to be 'sufficiently accessible to the individual who is affected by the restriction'. Censorship by algorithm is by definition not a transparent process meaning citizens will be deprived of the ability to understand how their speech online is being curtailed.

- **New powers for platforms such as Meta, Twitter, and even companies like Apple, will mean they may be performing functions of a public nature under the “Duty of Care” and could be subject to judicial review.** This is because content moderation will be brought under statute (as opposed to a private contract between user and platform), meaning restrictions on freedom of expression are imposed by a private body which is exercising public law functions and could therefore be subject to judicial review. This would represent a huge leap in the powers of technology companies, mandated by the Government. Users and platforms will need to 'lawyer up' in order to protect their voices online with complex legal interpretation and litigation required for them to be able to say online what is lawful to articulate in conversation at the pub.
- **The Secretary of State for Digital Culture Media and Sport will have an unparalleled ability to censor.** The Secretary of State will be given the power to guide how OfCom defines 'harmful content' arbitrarily, without sufficient democratic oversight - using the negative procedure for passing secondary legislation. This means a homophobic Secretary of State could have a statutory instrument passed censoring LGBTQ+ content within days and without full and proper Parliamentary scrutiny.
- **The proposal to proactively monitor private communications lack safeguards for journalistic or legally privileged material.** The Bill ignores the need for procedural safeguards to control and assess interference with established and recognised confidential information. Under the current legal framework this would include review by a judge or other independent and impartial decision-making body to refuse access where there is no overriding requirement in the public interest. This could make important everyday acts of journalism, such as securely speaking to a source, impossible.

The Government has ended up in this position having disregarded all the learnings from regulation of the online space over the last twenty years, including some of the fundamental

building blocks of the internet namely intermediate liability protections. This is despite pre-legislative scrutiny identifying flaws in the draft Bill.

In summary, the legal advice, published in full in this report, found:

- **The regime proposed by the Bill does not contain the statutory safeguards that would be required to prevent or limit the risk of violations of the right to freedom of expression.** The provisions incentivize and facilitate wide ranging interferences with free speech rights, without any obligation to assess them against legal criteria. Much content, or provision of/access to content, would be restricted without either a legitimate aim or where there is no pressing social need to do so. [see paragraph 56 of the Legal Opinion]
- **The structure of regulation offers no prospect of ‘fact-specific’ adjudications on speech,** meaning users will have to rely on platforms correctly interpreting and applying rules on a mass scale via algorithms. Those decisions will be based on OfCom’s interpretation of the new law and existing rights, inverting previous norms on permissible speech. [see paragraph 63 of the Legal Opinion]
- **Harmful speech has no legal basis and risks restrictions on speech that are too broad and therefore open to abuse through selective enforcement.** For example, there seems little prospect of allowing offensive and shocking content online when OfCom seeks to codify ‘harm’ at a later date - failing a key test on free speech. [see paragraph 36 of the Legal Opinion]
- **On the face of the Bill there appears to be a risk that platforms, and possibly Ofcom, may access confidential journalistic material in carrying out their statutory functions.** There is no recognition in the Bill of this possibility and no protection provided for the enhanced rights given under Article 10 ECHR to protect the confidentiality of such material. [see paragraphs 39 + 66 of the Legal Opinion]
- **‘Democratic importance’ protections are not as wide as existing human rights protections as they only cover a limited form of political expression.** Under ECHR definitions, this can include matters relating to parts of the world other than the particular European state in which the speech falls to be protected. However, the speech identified in clause 15 is limited to content specifically intended to contribute to democratic political debate in the UK. [see paragraph 65 of the Legal Opinion]

IN THE MATTER OF:

THE ONLINE SAFETY BILL

ADVICE

Introduction

- I am asked to advise 89up and Index on Censorship as to whether the legislative regime proposed in the Online Safety Bill (“the Bill”) would lead to violations of the right of internet users to freedom of expression under Article 10 of the European Convention on Human Rights (“ECHR”).
- The Bill seeks to regulate content on the internet in the UK. If enacted, it would do so by imposing legal requirements on certain providers of user-to-user services and search engines. These would require such regulated internet service providers (“ISPs”) to restrict the freedom of users to upload and access content online.
- The content in issue is broadly defined in the Bill. It falls into two principal statutory categories: illegal and harmful. The ISPs to be subject to the legal requirements will identify the content in these categories which is to be restricted. Because of the sheer volume of content on the internet they will do so, largely if not wholly, by using technology (such as algorithms, searches for particular words or phrases and so on).
- They will also determine what action to take to restrict the content once they have identified it. The actions envisaged in the Bill include taking down content and/or restricting users access to it. And taking action against users generating, uploading or sharing content (for example suspending or terminating their use of the service).
- The ISP’s compliance with the statutory regime will be overseen and enforced by the Office of Communications (OFCOM). The government would oversee, and would have powers to influence, how OFCOM performs these statutory functions.
- In my view the Bill, if enacted, will result in many violations of the right of freedom of expression of internet users under ECHR Article 10. This right is a “Convention Right” to which the provisions of the Human Rights Act 1998 apply (“the HRA”). So, domestic legislation must be drafted and applied in a way that ensures compliance with Article 10 principles. The Bill is not drafted in this way.
- This is my view for the reasons explained below.

- In order to avoid (or at very least minimize) this worrying prospect the Bill would have to be amended to recognize that the operation of its provisions will interfere with the Article 10 rights of users of the internet, through these sorts of restrictions. This should be its starting point. It does not do so in its current form. It would have to contain clear provisions protecting against restrictions being imposed on users which do not meet the strict criteria laid down by the European Court of Human Rights (“ECtHR”) for state interferences with the right to freedom of expression. These criteria are not acknowledged at all in the current draft of the Bill. There is only passing reference to the Convention in the Bill and it does not appear to contemplate that restrictions imposed by ISPs as a result of the legislation will amount to interferences with users Article 10 rights.

The Bill

- This is lengthy and complex. What follows is a brief summary of the most relevant provisions of the Bill. It is important that the workings of the Bill are understood, at least in outline, in order to understand the remainder of my advice.

Part 3

- The most important part of the Bill is Part 3 which contains nine Chapters. This imposes the key legal requirements on the regulated ISPs. These are called “*duties of care*” in the language of the Bill. But this should not obscure the fact that they are legal requirements of the state, imposed by statute, requiring the ISPs to act on behalf of the state to restrict freedom of speech.

Chapter 2

- This imposes duties of care on providers of regulated user-to-user services.
 - There are duties in relation to what the Bill describes as *illegal content*. This is either *priority* illegal content or *other* illegal content. All providers of these services must maintain assessments of the risks of users encountering illegal content on their services and the risks of harm from the same. They must also have *systems and processes* to take down priority illegal content and prevent users encountering it (by blocking it), and to take down any illegal content of which they become aware. The ISP must have terms of service specifying how users are to be protected from illegal content and must apply these consistently in relation to all content which the ISP *reasonably considers* to be illegal content.
 - Duties are also imposed in respect of *Category 1* user-to-user services. These will be the services with the most users. Providers must maintain an *adults’ risk assessment*. This is an assessment of the risk of adults

encountering *priority content that is harmful to adults* according to a designation regime under the legislation, and the level of risk of harm to adults from the same. The *safety duties* to protect adults include obligations to specify in the ISP's terms of service how it will *take down* and *restrict access to* priority content deemed harmful to adults or limit its *promotion* on the service. Again, the duty to apply terms of service protecting users from such content applies to all content that the ISP *reasonably considers* to be such content.

- There are also risk assessment and safety duties for services *likely to be accessed by children*.
- Clause 15 requires Category 1 services to have *systems and processes designed to ensure that the importance of the free expression of content of democratic importance is taken into account* when taking decisions about:
 - *how to treat such content (especially decisions about whether to take it down or restrict users' access to it)*;
 - whether to take action against a user who is generating, uploading or sharing it.

There is a duty to have and to apply terms of service protecting such content. But the latter only applies where the ISP *reasonably considers* the content to be of this sort. By clause 15(6)(b) *content of democratic importance* is limited to content which appears to be *specifically intended to contribute to political debate in the United Kingdom or a part or area of the United Kingdom*.

- Clause 16 requires Category 1 services to have *systems and processes designed to ensure that the importance of the free expression of journalistic content is taken into account* when taking decisions of the two types identified in Clause 15. The characterization of content as journalistic is left to the service provider. And, again, the duty only applies when taking decisions about content which the ISP *reasonably considers is journalistic content*. There is a limited and circular definition of *journalistic content* in Clause 16(8) according to which it is content: *generated for the purposes of journalism*; and must be *UK linked*.
- A general duty applies in respect of all user-to-user services to *have regard to the importance of protecting users' rights to freedom of expression within the law* when *deciding upon and implementing, safety measures and policies*.

Chapter 3

- Duties are imposed on providers of regulated search services to: maintain illegal content risk assessments; and to have *proportionate systems and processes designed to minimize the risk of* encountering priority illegal content and other illegal content which is known about. They must have a publicly available statement saying how they will protect individuals from search content that is illegal content; and they must apply the provisions of the public statement to search content that the *provider reasonably considers is illegal content*.

- There are risk assessment and safety duties for search services likely to be accessed by children.
- A general duty in relation to freedom of expression, in the same terms as clause 19(2) (ie in relation to implementing safety measures and policies) applies to regulated search services.

Chapter 6

- OFCOM is required to maintain published codes of practice in respect of the duties imposed on providers of Part 3 services, having consulted on the same. A code of practice may include a measure identifying use of proactive technology to analyse publicly communicated content/metadata as a way of complying with a duty. Before issuing a code, a copy must be provided to the Secretary of State for Digital, Culture, Media and Sport. If the Secretary of State does not give a direction to OFCOM to modify the draft, it will be laid before Parliament and is subject to the negative procedure.
- But the Secretary of State can direct OFCOM to modify the draft for *reasons of public policy*. OFCOM must then comply with the direction and resubmit a draft of the Code, modified as required by the minister. This modification procedure can be repeated. In the case of a modified code the affirmative procedure applies in respect of Parliamentary scrutiny.
- Clause 45(1) provides that a provider of a Part 3 service *is to be treated as complying with* a duty imposed on them under Chapter 2 or 3 of Part 3:

...if the provider takes or uses the measures described in a code of practice which are recommended for the purpose of compliance with the duty in question....

Chapter 7

- Clause 52 defines *illegal content* as content that amounts to a *relevant offence*. The offence may be: using the words, images, speech or sounds of the content; using the same *together with* other user generated content on a user-to-user service; possessing, viewing or accessing the content; or publishing or disseminating the content. There are four categories of relevant offence, namely specified terrorism offences, CSEA offences and *other priority offences*; and fourthly other offences where the *victim or intended victim is an individual or individuals*. The first three categories are *priority illegal content*.
- Clause 54 defines content that is *harmful to adults*. This is of two types.
 - Priority content that is harmful to adults: This is content *of a description designated* as such in regulations made by the Secretary of State;
 - Other content harmful to adults: This is content which presents *a material risk of significant harm to an appreciable number of adults in the United Kingdom*.

The Secretary of State may designate content as harmful by regulation only if they consider that there is such a *material risk* from such user generated content.

Part 7

- This sets out OFCOM's powers and duties. These include establishing a *register* of regulated Part 3 service providers. OFCOM can: require information from regulated ISPs to assess compliance with the Part 3 duties of care; investigate compliance with the Part 3 duties using powers to interview and enter/inspect; require regulated ISPs to use accredited technology to deal with terrorism content and/or CSEA content; and enforce compliance with Part 3 duties by requiring ISPs to take specified steps, including using proactive technology to enforce duties relating to illegal content/content harmful to children. It can impose financial penalties on non-compliant regulated ISPs. OFCOM can also apply to a court for orders to disrupt the business of non-compliant service providers.

Part 9

- This empowers the Secretary of State to make a statutory statement of the strategic priorities of the government in relation to online safety matters; and to issue guidance, to which OFCOM must have regard, about how they exercise their functions under the Act.

ECHR Article 10

- Article 10 provides:
 1. *Everyone has the right to freedom of expression. This right shall include freedom to hold opinions and to receive and impart information and ideas without interference by public authority and regardless of frontiers. This Article shall not prevent States from requiring the licensing of broadcasting, television or cinema enterprises.*
 2. *The exercise of these freedoms, since it carries with it duties and responsibilities, may be subject to such formalities, conditions, restrictions or penalties as are prescribed by law and are necessary in a democratic society, in the interests of national security, territorial integrity or public safety, for the prevention of disorder or crime, for the protection of health or morals, for the protection of the reputation or rights of others, for preventing the disclosure of information received in confidence, or for maintaining the authority and impartiality of the judiciary.*
- This is a qualified, not an absolute, right.

- Article 10.1 identifies the right. Applied to internet use the Art 10.1 right (the freedom to hold opinions and to receive and impart information and ideas *without interference* by public authority) can be asserted by those who seek to disseminate information and ideas via the internet by uploading content; and by those who want to access the content and read/view/listen to it (ie receive it).
- Article 10.2 explains how public authority may justifiably interfere with these rights (ie without causing a violation of the right).

These provisions have been considered many times over the years by the European Court of Human Rights (“ECtHR”) and by the courts in the United Kingdom. The principles that apply under these provisions have been identified in the case-law and are well-established.

- They include three particularly important general principles.
- First, the right applies:

...not only to “information” or “ideas” that are favourably received or regarded as inoffensive or as a matter of indifference, but also to those that offend, shock or disturb; such are the demands of that pluralism, tolerance and broadmindedness without which there is no “democratic society”...

(the “Handyside principles”).

- Secondly, the right protects all forms of expression and the form as well as the substance of the expression is protected. Thus, it protects for example images, verbal and non-verbal expression and all forms of conduct (such as conduct by way of protest and/or performance),
- Thirdly, Art 10.2 must be construed strictly and the necessity for any restrictions on freedom of speech which the state seeks to justify under Art 10.2 must be established convincingly on the facts of the particular case.

Article 10.1

- The right is “engaged” whenever there is an *interference* with it by *public authority*. This means that where there is an interference with the right within the meaning of Art 10.1, the state must justify the interference in the way envisaged by the provisions of Article 10.2. The requirements of Art 10.2 are considered below.
- The concept of *interference* by public authority under the Convention is closely connected with status to complain of a violation of Convention right. This is known as *victim* status. See ECHR Art 34. A person cannot claim to be victim of a Convention right where they are not *directly affected* by a domestic law. But they can claim to be directly affected by it (and so a victim) where they are directly affected by an individual measure of implementation of the law (eg against them or a group including them) or where the operation of the law requires them to modify their

behaviour to avoid such a measure. These are issues that fall to be decided on the facts of the particular case.

- It is well established that there can be an Article 10.1 *interference* where restrictions upon freedom of expression which are imposed by a private body which is exercising public law functions, for example functions provided for statute. In domestic law s.6(3) of the HRA is applied in deciding whether acts and/or omissions of a legal person or entity engage Convention rights. HRA s.6(3)(b) provides that a *person whose functions are functions of a public nature* must act compatibly with Convention rights. In applying this provision, our courts look closely at the nature of the functions undertaken by the entity, to see whether they are functions of a public nature. Critical factors will always be whether the activity in issue has its origins in governmental responsibilities and whether the statutory regime compels those asserting the Convention right to rely on the entity concerned for the realization of the right.
- Blocking access to the internet has been recognized by the ECtHR as an interference with the Art 10 right.

Article 10.2

- This imposes three requirements which the state must establish to show justification for the interference. First that the interference was prescribed by law; secondly that it pursued one or more of the listed *legitimate aims* in the second half of Article 10.2; and thirdly that it was *necessary in a democratic society*.
- The first is known as the principle of legality. It raises three distinct questions, identified by Lord Hope in **R v Shayler** [2003] 1 AC 247 thus:

[56]...The first is whether there is a legal basis in domestic law for the restriction. The second is whether the law or rule in question is sufficiently accessible to the individual who is affected by the restriction, and sufficiently precise to enable him to understand its scope and foresee the consequences of his actions so that he can regulate his conduct without breaking the law. The third is whether, assuming that these two requirements are satisfied, it is nevertheless open to the criticism on the Convention ground that it was applied in a way that is arbitrary because, for example, it has been resorted to in bad faith or in a way that is not proportionate...

The ECtHR has cautioned against restrictions on speech that are too broad and therefore open to abuse through selective enforcement. It has found that the principle of legality was not met where under domestic law *any opinion or idea that is regarded as offensive, shocking or disturbing can easily be the subject of investigation*. Where laws are inappropriately vague and the way in which they will be applied is difficult to foresee, the quality of law issue may be secondary to the question of whether such laws *are necessary as general measures*. The conclusion may be that they are open to abuse in individual cases and incompatible with the *notions of equality, pluralism and tolerance inherent in a democratic society*.

- As to the third requirement: there must be relevant and sufficient reasons to support the restriction on free speech in issue; the restriction must correspond to a *pressing social need*; and it must be proportionate to the legitimate aim being pursued. See Lord Hope in **Shayler** (above) at [58]. These are again matters that must be decided by reference to the facts of the case (especially the form and content of the expression in issue). Lord Hope went on to explain the matters that need to be considered *where a question is raised as to whether an interference with a fundamental right* such as the right to free speech is proportionate.

[61]...The first is whether the objective which is sought to be achieved—the pressing social need—is sufficiently important to justify limiting the fundamental right. The second is whether the means chosen to limit that right are rational, fair and not arbitrary. The third is whether the means used impair the right as minimally as is reasonably possible. As these propositions indicate, it is not enough to assert that the decision that was taken was a reasonable one. A close and penetrating examination of the factual justification for the restriction is needed if the fundamental rights enshrined in the Convention are to remain practical and effective for everyone who wishes to exercise them.

- In applying these principles the ECtHR and the domestic courts recognize three broad categories of speech. Though particular acts of expression can include elements of more than one of these. These are: expression on matters of general public concern; commercial expression; and artistic expression.
 - The highest importance attaches to expression in the first category. This means that particularly strong justification under Article 10.2 is required for state interferences with this type of speech. It includes political expression and it is well established that there is very little scope under Article 10.2 for restrictions on political speech. But it goes well beyond that, covering discussion of, and comment on, anything of public concern.
 - The ECtHR recognizes that satire is a form of artistic expression and social commentary which, by its inherent features of exaggeration and distortion of reality, naturally aims to provoke and agitate. Accordingly, the case-law requires that any interference with the right of an artist – or anyone else – to use this means of expression must be examined with particular care.
- Under Article 10 the press and other media (as well as NGOs) are recognized as having a special place in a democratic society, as purveyors of information and public watchdogs. Restrictions on the Article 10 rights of the media and individual journalists are particularly closely scrutinized under Article 10. Especially where the activities relate to matters of public concern. This protection covers the news and information gathering activities of journalists, not just their publications. Thus, the Article 10 right of journalists embraces a strong right to protect their confidential journalistic material and sources. The important features of this privilege are:
 - Acts of entities exercising statutory functions by which journalists are compelled to give up their privilege and provide information on their sources or by which access to confidential journalistic information is obtained constitute interferences with journalistic freedom of expression.

- Because of the importance that attaches to this journalistic privilege in a democratic society and the potentially chilling effect that enforced disclosure/obtaining of such information has on the exercise of journalistic freedom of expression such measures cannot be compatible with Article 10 of the Convention unless justified by an *overriding requirement in the public interest*. The *overriding public interest* must be made out in applying the facts of the case to the test of necessity in a democratic society under Article 10(2).
- It is sufficient for the source protection right to be engaged that the material in issue is capable of identifying the source/s (ie it does not have to directly identify the source/s itself).
- Any such interference with the right to protect such sources/journalistic material must be attended with legal procedural safeguards commensurate with the importance of the principle at stake. These must include review by a judge or other independent and impartial decision-making body. The independent reviewer should have all the relevant facts before them and apply the Article 10 case-law principles. And the reviewer should have the power to refuse access where there is no *overriding requirement in the public interest* requiring the right to be restricted.

In the recent decision of the Grand Chamber of the ECtHR in ***Big Brother Watch v UK*** the court ruled that where legislation led to acquisition of confidential journalistic information/data (especially source identifying material) as a “*bycatch*” of a bulk interception operation

...storage and examination by an analyst should only be possible if authorised by a judge or other independent and impartial decision-making body invested with the power to determine whether continued storage and examination is “justified by an overriding requirement in the public interest.”

Article 10 and use of the internet

- Recommendations of the Committee of Ministers are taken into account by the ECtHR and guide the development of the law under Article 10. Recommendation CM/Rec (2014) 6 of the Committee of Ministers to member States on a Guide to human rights for Internet users was adopted. The relevant part of the Recommendation stated:

3. The Internet has a public service value. People, communities, public authorities and private entities rely on the Internet for their activities and have a legitimate expectation that its services are accessible, provided without discrimination, affordable, secure, reliable and ongoing. Furthermore, no one should be subjected to unlawful, unnecessary or disproportionate interference with the exercise of their human rights and fundamental freedoms when using the Internet.

The relevant parts of the Guide stated:

Access and non-discrimination

1. *Access to the Internet is an important means for you to exercise your rights and freedoms and to participate in democracy. You should therefore not be disconnected from the Internet against your will, except when it is decided by a court. In certain cases, contractual arrangements may also lead to discontinuation of service but this should be a measure of last resort.*

Freedom of expression and information

You have the right to seek, receive and impart information and ideas of your choice, without interference and regardless of frontiers. This means:

1. *you have the freedom to express yourself online and to access information and the opinions and expressions of others. This includes political speech, views on religion, opinions and expressions that are favourably received or regarded as inoffensive, but also those that may offend, shock or disturb others. You should have due regard to the reputation or rights of others, including their right to privacy;*

2. *restrictions may apply to expressions which incite discrimination, hatred or violence. These restrictions must be lawful, narrowly tailored and executed with court oversight;...*

4. *public authorities have a duty to respect and protect your freedom of expression and your freedom of information. Any restrictions to this freedom must not be arbitrary, must pursue a legitimate aim in accordance with the European Convention on Human Rights such as, among others, the protection of national security or public order, public health or morals, and must comply with human rights law. Moreover, they must be made known to you, coupled with information on ways to seek guidance and redress, and not be broader or maintained for longer than is strictly necessary to achieve a legitimate aim ...”*

- The ECtHR has ruled that denial of access to the internet may give rise a violation of a person’s Art 10 rights.

Discussion and advice

- If the Bill is enacted, many further, important features of the regulatory regime it proposes will remain to be worked out before it comes into effect. Most notably regulations will have to be made describing/defining content which is *harmful* to adults (and children). OFCOM guidance codes of practice will remain to be promulgated. So will the Secretary of State’s strategic priority statement and guidance to OFCOM.
- But it is possible to identify the fundamental flaws in the proposed regime and the likely impact of the same, by close consideration of the proposed primary legislation.

Interferences with Article 10 rights

- The most important flaw is the failure of the Bill to recognize that the operation of the regime will lead to “*interferences*” with the Article 10.1 right, as this concept is understood in the law under Article 10.1.
- As CM/Rec (2014) 6 acknowledges, there can be circumstances in which, absent legislation, decisions under the terms of service of providers will lead to restrictions by ISPs on use of that service as a last resort. Currently this may include cases where ISPs acquire specific knowledge of illegal content hosted by them, for which they then become potentially liable. Here they lose their immunity from liability under the e-commerce Directive and may feel compelled, having been put on notice, to take down the material as being illegal.
- But if this legislative regime comes into force there will be very many more restrictions on internet use and, critically, these will be the result of the operation of the legislation. Rather than decisions made by ISPs as private entities providing a commercial service. Indeed, this is the whole point of the Bill. This is what it is setting out to achieve.
- The restrictions will result from the ISP’s, required to do so by the legal duties imposed on them under the regime, identifying, and acting to restrict access to, quantities of online content (identified by their technology as *illegal* or *harmful* content in the language of the Bill) and/or acting against those who create and upload it.
- The pressure to restrict that will be imposed on ISPs is apparent from the summary of the Bill above. The obligations to identify content considered objectionable under the regime are many and wide-ranging. So are the categories of content identified in the Bill. If ISPs appear to OFCOM to be falling short on their obligations to identify and restrict such content they can be investigated, forced to apply them more strictly and sanctioned if they do not. Codes of practice can be made yet more detailed/prescriptive. The attraction to ISPs of taking the measures prescribed in a code of practice are obvious. They will be deemed to have complied with the relevant duty if they do so.
- Pressure will come from the top down under the proposed statutory regime. The government can impose pressure on OFCOM as to how they direct the ISPs to carry out those duties in particular by requiring modifications to the codes of practice. Clause 40(1)(a) indicates a wide power in the Secretary of State to require changes to draft codes.
- The end result will be that many internet users will be directly affected by the law, either as a result of implementation measures taken by the ISPs under the law or because they will have to modify their behaviour (including self-censoring) to avoid such measures. In my view the analysis and conclusion are the same under the domestic law (ie applying HRA s.6(3)(b)). Where the acts/omissions of the ISP which interfere with the Art 10 right in play will be the result of the statutory duties imposed on them by the statutory regime, the ISP would have to act compatibly with the principles under Art 10 of the Convention. This will be so even if the ISP is acting against a user with whom it has a contractual arrangement. This is because the restriction on free speech will not be the consequence of any private arrangement with the user, but rather the result of the legislative regime imposed by government and overseen by OFCOM. Here the government must accept that, by making the

legislation, it has assumed responsibility for protecting citizens against online content it perceives to be harmful. So, the activity of the ISP will be one which has its origins in governmental responsibilities. The statutory regime will compel those exercising the Convention right of freedom of expression to rely on the decision making of the ISP for the realization of the right.

Compliance with Article 10.2 principles.

- The critical question then is, will ISPs identify and act against content and content providers only in a way that meets the strict conditions for justified state interferences with free speech under Article 10.2?
- The answer is, in my view, clearly no.
- This is not to say that there will not be very many cases in which an outcome under the legislative regime, involving an interference with Article 10 rights, will be justifiable under Article 10.2. Though these might, perhaps, sometimes be outcomes more by accident than by design. My concern is about the cases where this would not be the outcome.
- This is so for many reasons, again apparent from the proposed regime. It is not possible to discuss all of them in this Advice. But the key concerns are as follows.
- Most importantly, the regime proposed by the Bill does not contain the statutory safeguards that would be required to prevent or limit the risk of violations of the right. It is not drafted in a way that recognizes the risk of violations of the Article 10 right and that mandates ISPs to carry out their statutory functions in accordance with the important Article 10.2 principles identified above.
- In addition, the categories of potentially proscribed content and of the obligations imposed on regulated ISPs are very wide indeed.
 - That the former is the case is apparent from the very many examples of potentially *illegal* content under the Bill. Exactly what the designations of priority content *harmful to adults* will cover is not clear. But the statutory test for such content is vague and does not suggest a high threshold. This is that it *presents a material risk of significant harm to an appreciable number of adults*. This is very subjective and gives the Secretary of State much scope to designate content as harmful to adults. The residual *other content harmful to adults* category similarly gives ISPs wide powers to identify particular content as harmful to adults.
 - The ISPs and search engines can, and are encouraged to, act against content in each category even if it is not actually illegal or harmful to adults as defined under the statutory regime. They only need to *reasonably* consider it to be so.

These provisions incentivize and facilitate wide ranging interferences with free speech rights, without any obligation to assess them against Article 10.2 criteria. It seems obvious that much content, or provision of/access to content, would be

restricted under the proposed regime without either a legitimate aim and/or where there is no pressing social need to do so.

- The lack of precision in the Bill when it seeks to identify content that may be restricted is also of great concern. It leaves open the strong possibility of challenges to the implementation of the proposed regime identifying a failure to respect the principle of legality. This is most obviously so in relation to the identification of content *harmful to adults* provisions in clause 54.
 - As drafted the residual category is, in my view, too broad and therefore open to abuse through selective/arbitrary enforcement by ISPs. This is because the underlying concept of *harm* from internet speech is inherently vague. It cannot, by definition, connote physical damage and so, presumably, must connote some form of unspecified mental damage. But the Bill does not define or limit the mental damage in issue. And the risk of such harm resulting is placed at an extremely low level, again vaguely expressed – ie merely a material risk of significant harm to an appreciable number of adults (emphasis added);
 - It is possible that the regulations designating some content as *priority* content harmful to adults, will identify categories of such content more precisely. But even this seems unlikely. The designation is only to be by *description* of the content. The content will still have to present the same risk. There will also be much scope for challenges to the lawfulness of particular descriptive categories of content (ie as not meeting the statutory *material risk of significant harm to an appreciable number of adults* condition for identifying such content by description).

Indeed, in my view this aspect of the legal regime will inevitably be so vague that the quality of law issues will be secondary to the question of whether such a law is necessary as a general measure. It is difficult to see how it is, given the extent to which legitimate/protected speech will be wrongly restricted and the tendency that such a law will have to chill such expression on the internet.

- There is no suggestion anywhere in the Bill that there will be a *close and penetrating examination of the factual justification* for restrictions, of the sort identified by Lord Hope in **Shayler**. Quite the contrary is the case. The third requirement under Article 10.2 (that the restriction is *necessary in a democratic society*) requires nuanced and evaluative judgments to be made on the facts of each individual case. This is particularly so where the important Handyside principles are in play and latitude has to be given to speech that many might regard as offensive, shocking or disturbing.
- There is no realistic prospect of such judgments being made properly and consistently by technology. Or indeed by employees of ISPs.
- Obvious examples of where this will be problematic are assessments of potentially *illegal* content or of satirical content (which lends itself to being wrongly assessed by technology as either *illegal* or harmful).
- To take one possible example of possible *illegal* content. Section 13(1A) of the Terrorism Act 2000 is a listed offence in Schedule 5. It criminalises publication of an

image of something (an “*article*”) *in such a way or in such circumstances...as to arouse suspicion* that a person is a supporter of a proscribed organisation. This could be tee shirt or a badge or a banner with text. A police officer or prosecutor would have to make difficult decisions, assessing the article, identifying a particular proscribed organisation and then assessing any apparent link between the *article* appearing in the image and the organisation. The chances of technology or an ISP employee making the right decision in such cases are remote. The other listed offences are mostly similarly difficult to judge, even for prosecutors and police. In the 21st century statutory criminal offences tend to be identified in pieces of dense, complex drafting.

- The absence of any recognition of the risk of violations of the Article 10 right, and any requirement for ISPs to carry out their statutory functions in accordance with Article 10.2 principles, is most concerning however in relation to the *harmful to adults* category.
- The elusive nature of this category means that a particularly *close and penetrating examination of the factual justification* for any restriction would be required. The legitimate aim/s to be pursued might be appropriately identified as protection of health or morals, or of the rights of others. But in the vast majority of cases, it would be impossible for an algorithm or an employee of an ISP to evaluate properly whether there was a pressing social need to act against such content in pursuance of such an aim or whether a particular restriction was proportionate. Even if such an evaluation were mandated under the legislation, which it is not. In these cases, such an evaluation would challenge a professional judge with all the relevant evidence before them. Under this regime the decision-taking process would be far removed from this sort of exercise.
- It is already well understood that content moderation by ISPs adversely affects certain groups disproportionately. There are well known examples of content relating to LGBTQ sexual health or women’s health being restricted. And content in Arabic or Urdu is more likely to be restricted than English language content. The risks of such unjustifiable outcomes being multiplied if the regime includes this category are obvious. Such outcomes are clearly incompatible with notions of equality, pluralism and tolerance inherent in a democratic society.

Clauses 15 and 16

- Clause 15 purports to give some greater protection, where it applies, to content of *democratic importance*. But its value in protecting rights to freedom of expression will be limited. This is because it does not mandate strong protection, as under Article 10, for expression on all matters of general public concern. Under the Strasbourg case-law this is a fact sensitive, open-ended category and is not limited to expression about matters of such concern to do with events in the United Kingdom. It can include matters relating to parts of the world other than the particular European state in which the speech falls to be protected. The type of speech identified in clause 15 is, by contrast, very limited. It covers only expression *specifically intended to contribute to democratic political debate* in the UK.
- Clause 16 purports to give some greater protection, where it applies, to *journalistic content*. But its value is, similarly, extremely limited. It does not mandate protection in

principle for all journalism, or even all journalism of public interest value. It only covers what is reasonably considered to be *UK-linked* journalism. This requires that UK users of the service are the or a target *market* for the content and that the content is *likely to be of interest to a significant number of UK users*. This severely restricts the value of this provision in protecting online speech.

Clauses 19(2) and 29(2)

- These impose an indistinct duty to have regard to the importance of protecting: *users' right to freedom of expression within the law; the rights of users and interested persons to freedom of expression within the law*. It is not clear what right is being referred to in these clauses. But they appear to reflect the old common law maxim that a citizen can say anything provided it is not prohibited by law. It is certainly not a reference to the Article 10 right which is fundamental, supranational human right that is not dependent on compliance with domestic laws. The value of these provisions in protecting free speech online is again extremely limited. They do not mandate presumptive protection for the right to a wide freedom of speech, which can only be restricted in clearly defined, limited circumstances, in the way Article 10 does.

Confidential journalistic information

- It is difficult to predict how the use of technology encouraged (and in some cases to be required) under the proposed statutory regime will affect the rights of journalists to protect their confidential information/sources. On the face of the Bill there appears to be a risk that ISPs, and possibly OFCOM, may access such material in carrying out their statutory functions. There is certainly no recognition in the Bill of this possibility and no protection provided for the enhanced rights given under Article 10 to protect the confidentiality of such material. In my view there should be. These should be statutory safeguards that meet the requirements of the **Goodwin, Sanoma** and **Big Brother Watch** line of authority discussed above. These principles are clear, well-established and specific to this right. Clauses 15, 16, 19(2) and 29(2) would not provide the required protection for these rights because they are not drafted with Article 10 or these rights in mind. This is another matter of concern. And another potential route to violations of Article 10 rights.
- I would be happy to discuss the contents of this Advice and any matters arising out of them with my clients.

GAVIN MILLAR QC

Matrix

Key Recommendations

The Bill requires a ‘free speech health check’ through the Committee Stage in Parliament to protect against restrictions being imposed on users which do not meet the strict criteria laid down by the European Court of Human Rights for state interferences with the right to freedom of expression.

- **Protecting freedom of expression**

Section 19 of the Bill sets out companies’ duties to protect Freedom of Expression in relation to user-to-user services. **The duties, as currently drafted, are quite broad and vague.** The protections need to be strengthened. It needs to be beefed up so that social media companies have a proper set of competing duties that need to be balanced. **We should ensure Freedom of Expression duties are legislated for in a far more explicit way** through express provisions for protected characteristics (legal speech by minority groups such as religious groups women/ethnic minorities/LGBTQ/disabled. This model is analogous to Religious Organisations’ carve out on gay marriage in the [Marriage \(Same Sex Couples\) Act](#).

Enhanced rights to freedom of expression

19 Duties about freedom of expression and privacy

(1) This section sets out the duties about freedom of expression and privacy which apply in relation to regulated user-to-user services as indicated by the headings.

The duties about rights to freedom of expression and privacy in relation to user-to-user services, as referred to in this section, are.

All services

(2) A duty to have regard to the importance of—

(a) protecting users’ right to freedom of expression within the law, Including (but not limited to) the protected characteristics of ethnic minority communities, LGBTQ+ communities, and persons with disabilities and

(b) protecting users from unwarranted infringements of privacy, when deciding on, and implementing, safety policies and procedures.

(c) protecting users' right to freedom of religion

(d) protecting users' right to liberty and security

(e) protecting users' right to freedom of thought and conscience

(f) protecting users' right to freedom of assembly and association

(g) protecting users' right to life

(h) protecting users' right to freedom of press

(i) protecting users' right to freedom of petition

(j) protecting users' right to freedom from unreasonable searches and seizures

- **Removing Legal But Harmful speech**

Removal of the Duty of Care and all reference to its structure in sections 5 and 6 of the Bill would fundamentally ensure that speech online was treated the same as speech offline. **If the Duty of Care is not removed, it should at the very least be amended** to apply to effect illegal content only (as set out by the Lords Committee in their report) and 'legal but harmful' content should be excluded from the duties that require codes of practice.

Amendments Proposed

Part 3 — Providers of regulated user-to-user services and regulated search services: duties of care

Chapter 2: Providers of User-to-User services: Duties of Care

13 Safety duties protecting adults

(1) This section sets out the duties to protect adults' online safety which apply in relation to Category 1 services.

(2) A duty to summarise in the terms of service the findings of the most recent adults' risk assessment of a service (including as to levels of risk and as to nature, and severity, of potential harm to adults).

(3) A duty to include provisions in the terms of service specifying, in relation to each kind of priority content that is harmful to adults, that is to be treated in a way described in subsection

(4), which of those kinds of treatment is to be applied.

(4) These are the kinds of treatment of content referred to in subsection (3)—

(a) ~~taking down the content;~~

(b) ~~restricting users' access to the content;~~

(c) limiting the recommendation or promotion of the content;

(d) recommending or promoting the content.

(5) A duty to explain in the terms of service the provider's response to the risks relating to priority content that is harmful to adults (as identified in the most recent adults' risk assessment of the service), by reference to—

(a) any provisions of the terms of service included in compliance with the duty set out in subsection (3), and

(b) any other provisions of the terms of service designed to mitigate or manage those risks.

(6) If provisions are included in the terms of service in compliance with the duty set out in subsection (3), a duty to ensure that those provisions—

(a) are clear and accessible, and

(b) are applied consistently in relation to content which the provider reasonably considers is priority content that is harmful to adults or a particular kind of priority content that is harmful to adults.

(7) If the provider of a service becomes aware of any non-designated content that is harmful to adults present on the service, a duty to notify OFCOM of—

(a) the kinds of such content identified, and

(b) the incidence of those kinds of content on the service.

(8) In this section—

“adults’ risk assessment” has the meaning given by section 12;

“non-designated content that is harmful to adults” means content that is harmful to adults other than priority content that is harmful to adults.

(9) See also, in relation to duties set out in this section, section 19 (duties about freedom of expression and privacy).

- **Illegal content thresholds**

The test for **illegal content should be ‘actually’ illegal, not that platforms have ‘reasonable grounds to believe’ content is illegal**. The reason why this change is needed is that platforms will interpret their ‘reasonable belief’ widely and depending on the political circumstances of the speech concerned, will not want to be blamed or fined for content remaining online. This will inevitably lead to over-censorship and there are currently insufficient free speech safeguards against such platform behaviour.

The test of ‘actual knowledge of illegality’ meets the criteria in the E-commerce regulations which is already applied to the law of libel. **Aligning this criteria with pre-existing criteria already in use in other areas of law**, which have proven to be adequate and efficient, would ensure the law is effective and certain.

Amendments Proposed

Chapter 2 - Providers of User-to-User services: Duties of Care

Part 3 - Providers of regulated user-to-user services and regulated search services: duties of care

9 Safety duties about illegal content

(1) This section sets out the duties about illegal content which apply in relation to all regulated user-to-user services.

(2) A duty, in relation to a service, to take or use proportionate measures to effectively mitigate and manage the risks of harm to individuals, as identified in the most recent illegal content risk assessment of the service.

(3) A duty to operate a service using proportionate systems and processes designed to—

(a) prevent individuals from encountering priority illegal content by means of the service;

(b) minimise the length of time for which any priority illegal content is present;

(c) where the provider is alerted by a person to the presence of any illegal content, or becomes aware of it in any other way, swiftly take down such content.

(4) The duties set out in subsections (2) and (3) apply across all areas of a service, including the way it is operated and used as well as content present on the service, and (among other things) require the provider of

a service to take or use measures in the following areas, if it is proportionate to do so—

- (a) regulatory compliance and risk management arrangements,
 - (b) design of functionalities, algorithms and other features,
 - (c) policies on terms of use,
 - (d) policies on user access to the service or to particular content present on the service, including blocking users from accessing the service or particular content,
 - (e) content moderation, including taking down content,
 - (f) functionalities allowing users to control the content they encounter,
 - (g) user support measures, and
 - (h) staff policies and practices.
- (5) A duty to include provisions in the terms of service specifying how individuals are to be protected from illegal content, addressing each paragraph of subsection (3), and (in relation to paragraphs (a) and (b)) separately addressing terrorism content, CSEA content (see section 52 and Schedule 6) and other priority illegal content.
- (6) A duty to apply the provisions of the terms of service referred to in subsection (5) consistently in relation to content which the provider ~~reasonably considers~~ has sufficient evidence that is illegal content or a particular kind of illegal content.

EXPLAINER - who will be impacted by the draft Online Safety Bill?

The short answer is almost everyone who uses the internet. The vague nature of the Bill means that it is anticipated it will touch on every single UK user of social media, search engines and other platforms 'within scope'. A single misconstrued post or an overzealous algorithm could lead to severe consequences on how UK citizens communicate with friends and family and store precious memories. **In addition, we believe there are certain groups that will be particularly affected:**

VICTIMS OF CRIME To prosecute criminals for online wrongdoing, law enforcement agencies require access to the relevant content to use as evidence. If social media companies unilaterally delete illegal content without a proper system for archiving evidence, it will make the job of law enforcement much harder and by extension make all of us less safe.

JOURNALISTS Many journalists rely on social media messaging services to securely communicate with their sources. The Bill will allow the scanning of private communications which will fundamentally alter the confidential nature of the relationship between journalist and source and make important everyday secure communication impossible.

MEDIA ORGANISATIONS The Bill only mandates protection for content that is 'likely to be of interest to a significant number of UK users' and that is 'reasonably considered to be UK-linked journalism'. This means that content from international publications could be censored arbitrarily and be removed from social media platforms before appeals are lodged by these publishers.

UNIVERSITIES AND STUDENTS University students will be unable to debate important topics online, which is particularly problematic in the era of remote learning. Ironically, the Bill has been introduced at the same time as legislation aiming to protect free speech on campus. As noted by the Open Rights Group, "an incendiary speaker could deliver a provocative talk in a university lecture hall, and the university would be required to uphold his/her right to freedom of expression... [But] service providers may be required to remove that same speech [from the internet] as being subjectively harmful."

MARGINALISED PEOPLE At Index, we have already seen Artificial Intelligence used by tech platforms lead to the silencing of marginalised groups. Many marginalised communities have reclaimed words that were traditionally used as slurs against them, but the inability of AI to distinguish context means these posts will be removed as hate speech. Victims of trauma will be unable to share their own experiences online and get support as references to such topics could be considered potentially harmful.

LGBTQ+ COMMUNITY With censorship of LGBTQ+ content - such as essential educational content covering sexual health - already at a record high due to flawed AI and existing restrictive policies, this legislation would see huge amounts of perfectly legal content by LGBTQ+ users censored from the majority of the public, isolating them even more.

COMEDIANS The tendency of social media platforms to overcensor, coupled with AI's inability to recognise context, will mean that millions of ordinary people will find their jokes taken down and their accounts potentially suspended over remarks that were intended to be humorous or satirical.

SMALLER PLATFORMS The Bill could damage smaller platforms - for example on Mumsnet, there are thousands of conversations every day where women reach out for support after experiencing sexual abuse, or discovering that their kids are struggling with self-harm or eating disorders. Blanket definitions of subjects like these as 'legal but harmful' could force Mumsnet to shut those conversations down, and leave users without support.

PEOPLE LIVING UNDER DICTATORSHIP The Bill sets a dangerous international precedent on free speech online that will legitimise censorship and could be copied by autocrats globally to silence their opponents and citizenry.

MAY 2022.