A brief critical analysis of the Online Harms White Paper 2020

Dr. Francis Graydon

April 2021

In April 2019, the UK Government published its 'Online Harms White Paper' (OHWP).[1] The executive summary highlights two broad inter-related objectives. Firstly, to make the 'UK the safest place in the world to go online (relevant to users of digital services),[2] and secondly, 'the best place to start and grow a digital business'.[3] To achieve these ambitious goals, the government proposes an equally ambitious plan to exert greater control over "online harms" through the regulation of technology companies.

The government's conclusion is that 'the digital economy urgently needs a new regulatory framework 'to improve our citizens' safety online'.[4] The urgency for regulation is the government's response to: (i) the pressing need to tackle *illegal and harmful content online*; and (ii) the degree of public concern expressed about it in the UK and internationally. The UK initiative is not unique. In December 2020, the European Commission unveiled proposals for the Digital Markets Act (DMA) and the Digital Services Act (DSA). The DSA aims to build an EU-wide framework on the handling of illegal or potentially harmful content online and the liability of online intermediaries for third party content.

The UK proposal is promoted as a win-win for everyone. Overseen by an independent regulator, in-scope companies can look forward to greater clarity in knowing what is expected of them 'to keep their users safe' especially in the context of harmful content. [5] The framework will help 'citizens to 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'.[6] The regime is predicted to renew 'public confidence and trust in online companies and services'.[7] The regulator will set safety standards backed up by specific reporting requirements and enforcement powers.

[1] Department for Digital, Culture, Media and Sport, and the Home Office, *'Online Harms White Paper'* (2019) CP 57.

[2] Ibid. 5.

[3] Ibid. 5.

[4] Ibid*. 5.*

[5] Ibid*. 5.*

[6] Ibid. 5.

[7] Ibid. 5.

Concept of harm(s)

The proposal introduces an unusually broad scope of targeted online harms (harmful content and activity). The harms are based on evidence of their negative impact or influence on individuals and on society at large.[8] However, the evidence in support is less than robust. [9] Unhelpfully, no clear definition of harm is included. The government is 'consulting on definitions of private communications' [10] with respect to privacy in the framework but is silent on one for harm. The approach taken is based on a starting list of *harms* categorised as: 'harms with a clear definition', 'harms with a less clear definition', and 'underage exposure to legal content'.[11]

The paper highlights that the *harms* list is 'neither exhaustive nor fixed', thereby allowing for 'swift regulatory action to address new forms of online harm'.[12] This approach offers flexibility but is problematic. Firstly, in using an open-ended list approach, the concept of harm is clearly unbounded and subjective in nature.[13] It follows that the regulator will determine what legal content and activity ought, and ought not, to be deemed harmful and be regulated. Secondly, it also follows that the determination of the threshold to be applied by the regulator to trigger regulatory control of any "new harm", is also idiosyncratic in nature. The consequence is at best, uncertainty both for in-scope companies and service users, and at worst, self-censorship by users.

A third problem arises with the harms in the three categories. For example, the first

[8] Ibid. 42

[9] See V Baines, *'Online Harms and Folk Devils: Careful Now'* 24th June 2019. Available at https://medium.com/@vicbaines/on-online-harms-and-folk-devils-careful-nowf8b63ee25584, last accessed on 17 April 2021.

[10] Above n 1, 8.

[11] Above n 1, 31.

[12] Above n 1, 30.

[13] See G Smith, '*Online Harms White Paper- Response to consultation'* 28th June 2019. Available at https://www.cyberleagle.com/2019/06/speech-is-not-tripping-hazard-response.html, last accessed on 17 April 2021.

category (harms with a clear definition) (e.g., child sexual exploitation and abuse, sale of drugs, and harassment) constitutes illegal activity under existing laws in the offline world and is already prosecuted through criminal proceedings.[14] In-scope companies can continue to provide evidence and co-operate as part any police investigation or prosecution. Therefore, it is not strictly necessary for illegal activities to be incorporated into the proposed framework.

The second category (harms with a less clear definition) refers to generalised types of online content including 'disinformation', 'trolling', 'extremist content and activity' and 'intimidation', described as being 'problematic'.[15] However, these activities are not currently illegal. Regulating illegal and legal activities in the way proposed treats the categories as being directly comparable when they are not. It also asserts a similar level of discussion on their acceptability when none exists.[16] This "one size fits all" approach of combining the categories is problematic. It is compounded by empowering the regulator with what is described as a 'blank cheque' to determine what online lawful content and activity is 'harmful'.[17]

General test for harmful content or activity

In Dec 2020, following the White Paper consultation, the government proposed what can be described as a definition or "general test for harmful content and activity".[18] For content and activity to be "harmful" it must give rise to a *'reasonably foreseeable risk of a significant adverse physical or psychological impact on individuals'*.[19] The focus is now on personal safety.

[14] Ibid.

[15] Above n 1, 20.

[16] Above n 9.

[17] Big Brother Watch, *'Big Brother Watch's response to the Online Harms White Paper Consultation'* 12, July 2019. Available at https://bigbrotherwatch.org.uk/wp-content/uploads/2020/02/Big-Brother-Watch-consultation-response-on-The-Online-Harms-White-Paper-July-2019.pdf, last accessed on 17th April 2021.

[18] Department for Digital, Culture, Media and Sport, and the Home Office, '*Online Harms White Paper: Full Government Response to the consultation'* (2020) CP 354.

[19] Ibid. 24

While this test is better than an undefined notion of harm and provides greater clarity, it does raise other issues. Firstly, there is no detail about what constitutes 'significant adverse physical or psychological impact' and whether medical evidence of a psychological condition is required. Secondly, because psychological impacts are variable and subjective, there is a danger that this may lead simply to a threshold or standard based on the 'most readily upset or easily offended' user.[20] Thirdly, no significant detail about the operation of the test is provided. The framework emerging has a regulator with seemingly unfettered discretion to decide what constitutes an online harm and whether the test of harm is met.

An online statutory duty of care

The introduction of a new statutory duty of care is key in the new framework. Although changes to the scope of the duty were also proposed in December 2020 following the harms test above, it is important to first analyse how it operates before examining the effect of the changes.

The statutory duty is intended *'to make companies take more responsibility for the safety of their users and tackle harm caused by content or activity on their services.'* [21]. The duty will apply to social media platforms and a wide range of other internet companies that 'allow users to share or discover user-generated content or interact with each other online'.[22] It will apply to illegal and legal but harmful content and activities deemed harmful included in the categories above. The duty will extend from internet search engines, file sharing sites, customer review sites, public discussion, to messaging providers, cloud hosting providers, and others.

The duty will be overseen and enforced by the regulator (now OFCOM). OFCOM will set out codes of practice on *how* in-scope companies are expected to discharge the new duty. 'The codes will outline the systems, procedures, technologies and investment, including in staffing, training and support of human moderators, that

[20] Above n 13, 10.

[21] Above n 18, 26.

[22] Above n 1, 8.

companies need to adopt to help demonstrate that they have fulfilled their duty of care to their users.'[23] OFCOM will have the legal power to fine for non-compliance. The use of a statutory duty in the proposed regulatory model is novel. Legal experts and scholars are divided on whether this is the correct approach to "online harms". Woods contends that the statutory duty approach is appropriate and points to the extension and development of the principle in safety-related statutes in the Occupiers Liability Act 1957 and the Health and Safety at Work Act 1974 (HSWA).[24] Smith however maintains that the proposed framework is flawed because it ignores existing legal principles and cannot therefore function in the same way as safety related duties of care in the offline physical world.[25]

Secondly, there is also concern about the consequences of OFCOM enforcing the statutory duty. [26] Regulating the online activities of millions of users on a range of social media platforms will provide the regulator with a mechanism to censor and control free speech while regulating legal activity deemed harmful. It is appropriate to first examine the statutory duty model before turning to the issues raised in relation to free speech.

The proposed statutory duty of needs to be considered against the existing duty of care principle to determine whether it is appropriate. Under the proposed framework, there will be no individual right of legal action for any breach of the duty as in common law tort. Instead, enforcement of the duty of care will be by the regulator. Users will have no legal entitlement to compensation for duty breaches. This appears to be a limitation and weakness in the framework. However, Woods advances several reasons in support of the statutory duty model including: (i) previous legislation; (ii) flexibility for online environment; and (iii) focus on processes managing risks. [27]

[23] Above n 1, 42.

[24] See L Woods, '*The duty of care in the Online Harms White Paper*', 24 Sep 2019. Journal of Media Law, 11:1, 6-17. Available online at https://doi.org/10.1080/17577632.2019.1668605, last accessed on 1 April 2021.

[25] Above n 13, 2.

[26] Above n 13, 6.

[27] Above n 24 14-17.

(i) Previous legislation

The constitutional doctrine of the supremacy of Parliament means it is not restricted by the rules set down in tort introducing new legislation.[28] The duty of care principle has developed to address different contexts resulting in new laws. The principle from Donoghue v Stephenson within the common law doctrine of negligence,[29] is to exercise reasonable care and/or skill to avoid the risk of injury to others.[30] The duty is not against all risks and the courts have been guarded in extending the duty to novel situations.[31]

However, this duty has been extended through legislation to tackle irregularities and flaws in the duty scope. In the Occupiers Liability Act 1957, Parliament introduced a 'common duty of care' by imposing statutory duties of care upon property owners or occupiers as regards people using their places. This extended safety obligations on occupiers to see that visitors would be reasonably safe in using the premises for the purposes for which they were invited or permitted by the occupier to be there.[32] The Act changed the rules relating to existence of a duty of care, but did not alter the nature of the underlying cause of action.

In the proposed framework, there is the assumption of an online-offline equivalence. In the same way that offline property owners or operators have a duty to see visitors are reasonably safe, in-scope companies will be responsible in the same way for their online "public space". When an individual is online, they should be protected from harm in the same way through a duty of care imposed on the online provider. This has an attractive simplicity.

[28] AV Dicey, *'An Introduction to the Study of the Law of the Constitution*' 8th edn, Macmillan (1915) 37–38.

[29] *Donoghue v Stevenson* [1932] AC 562 (HL).

[30] *Bourhill v Young* [1943] AC 92 (HL), paras 98 and 104.

[31] Above n 24, 7.

[32] Under S. 2(2) of the Occupiers Liability Act 1957 (as amended) the obligation is to take 'such care as in all the circumstances of the case is reasonable to see that that person will not suffer injury or damage by reason of any such danger'.

Furthermore, Parliament imposed a statutory duty of care on employers as regards employees in the work environment with the Health and Safety at Work Act 1974 (HSWA). The safety related duties are broadly interpreted in terms of: (i) harms which employers should take steps to address; and (ii) the persons to whom the duties are owed.[33] Here the statutory duty is about systems that prevent problems and risks arising and to mitigate the consequences. The standard of the duty is one of reasonableness and related to the common law duty of care. The HSWA is also enforced by a regulator who not only performs an enforcement role, but also gives advice and sets standards.[34]

(ii) Flexibility

The scale of online systems is vast. This it makes it difficult to monitor and control their use on an individual basis. The online environment is viewed as 'fundamentally different from television and radio in its nature, audience and scale'.[35] OFCOM has indicated that any regulatory focus should be on 'the effectiveness and timeliness with which platforms take action to address harmful content'.[36] Faced with these challenges, a framework based on a statutory duty offers flexibility. The statutory duty within the HSWA model operates in many different environments (size and activity) and offers flexibility in the online environment.[37]

(iii) Goal-oriented systems and processes

The imposition of a statutory duty focuses on outcome and goal-orientated processes. It leaves the details of the solutions appropriate for the context on those who are subject to the duty placed HSWA. The regulatory framework is focused on; (i) identifying and assessing risks and identifying appropriate responses and (ii) preventing harm.

[33] Above n 24, 9.

[34] Above n 24, 9.

[35] OFCOM, Addressing harmful online content A perspective from broadcasting and on-demand standards regulation 25 https://www.ofcom.org.uk/__data/assets/pdf_file/0022/120991/Addressing-harmful-online-content.pdf, last accessed on 17 April 2021.

[36] Above n 35, 26.

[37] Above n 24, 11.

The imposed duty is not prescriptive of specific steps that must be taken. Rather the steps must be reasonably aimed at achieving an outcome. So in the same way, in-scope companies in the proposed regulatory model will be obligated to identify and assess online risks and identify appropriate responses.

Criticisms of statutory duty of care approach

Smith is particularly critical of the rationale behind the proposed statutory duty of care. It departs profoundly from established legal principles that underlie existing safety-related duties of care (statutory and common law) and is fundamentally flawed.[38] The proposal creates a 'broad duty of care' to promote some online behaviours while inhibiting others deemed harmful.[39] This "one size fits all" approach is unusual because is departs fundamentally from the norm of 'subject-specific legislation'.[40] Smith's second criticism is that the proposal ignores existing policy reasons and case law aimed at limiting a duty of care.[41] A third related criticism is that the proposal fails to spell out exactly how the duty will operate in the face of the existing principles and this relevant case law.[42]

The ordinary duty of care can be understood in simple terms as acting to avoid causing harm to an individual. The duty is not to prevent someone else from inflicting it. Smith[43] reminds us that the UK supreme court considered the existence and extent of the duty of care in Robinson v Chief Constable of West Yorkshire Police [2018] UKSC 4. The court highlighted that, *'private individuals and bodies, are generally under no duty of care to prevent the occurrence of harm'* [paragraph 34], and *'private individuals and bodies, generally owe no duty of care towards individuals to prevent them from being harmed by the conduct of a third party'* [paragraph 37].

However, contrary to the court's observations here, the statutory duty will extend to the online conduct of *third parties* and not the conduct of the intermediaries.

[38] Above 13, 2.

[39] Above 13, 9.

[40] Above 13, 3.

[41] Above 13, 2.

[42] Above 13, 2.

[43] Above 13, 2.

The duty imposes an obligation on the in-scope companies to prevent harm arising from the online activities and content of third-party users. The proposal does appear fundamentally flawed because the operation of the well-established legal principles, and the supreme court's conclusions about the limits of the duty is ignored or misunderstood. Despite this hurdle, there is a strong precedent for developing the duty principle through statute. In addition, the rationale and advantages of the statutory duty approach is clear. However, this "third-party" problem that arises is a significant issue. Neither the introduction of the definition or "general test for harmful content or activity" or the differential duty of care addresses the problem. In the end, the court may have to determine the issue.

Does the proposal strike a fair balance between the interests of the relevant stakeholders?

The introduction of the proposed regulatory regime may come with a range of potential risks and benefits for government, in-scope companies, the individual and society at large. One key question is whether the proposed regulation can really tackle online harms without damaging online freedom of expression. Freedom of expression is protected under the European Convention on Human Rights (ECHR) and any restrictions or censorship on free expression would need to meet the ECHR test of proportionality, legality, and necessity in a democratic society.[44]

One obvious concern is that the regulatory process will inevitably result in the suppression or censorship of lawful online content such as the freedom of expression about every online subject manner but particularly expression from unorthodox or dissenting voices. A second related concern is that depending on the political climate, the mechanism would be proactively deployed to achieve this. The third concern is the risk that in-scope companies will act over cautiously to avoid harsh financial sanctions

[44] T Mendel, '*A Guide to the Interpretation and Meaning of Article 10 of the European Convention on Human Rights'* (Council of Europe 2017) 39. Available at https://rm.coe.int/16806f5bb3, last accessed 1st April 2021.

leading to a ‘significant chilling of freedom of expression’.[45] OFCOM is expected to issue codes of practice about content that is specifically ‘not necessarily illegal’ but that may ‘directly or indirectly’ cause “harm” to other users.[46] The obvious danger here is that an unelected regulator will be determining, on an ongoing basis, what constitutes free speech in the online environment. Introducing limitations on an individual’s right to freely express themselves can only properly be decided by parliament. Permitting a state appointed regulator to interfere with this process would be undemocratic and potentially contravene Art 10 of the ECHR. Additionally, a lot of the Article 10 case law from the European Court of Human Rights (ECHR) concerns "high value" speech that contributes to discussion of matters in the public interest.[47] Low level ‘digital speech’ would fall into this category and would not be protected.[48]

Overall, given how the regime will operate it is difficult to conclude that a fair balance is achieved for the individual. The existing relational asymmetries will likely change in favour of in-scope companies. However, given the emphasis on “process” in the regime, individual cases of harm become less important, and the framework falls short of establishing any new right in favour of the individual for breaches.

What are the risks and benefits of “private policing” of online content?

The notion of “private policing” or self-regulation is one alternative to state intervention. It is important to make powerful in-scope companies more accountable to users in the methods used to host online content. This is especially so given the asymmetric relationship they have with their users, and lack of transparency around data

[45] D Tambini, *‘The differentiated duty of care: a response to the Online Harms White Paper’* (2019) Journal of Media Law, 11:1, 28-40, DOI: 10.1080/17577632.2019.1666488.

[46] Above n 1, 68.

[47] J Rowbottom, *‘TO RANT, VENT AND CONVERSE: PROTECTING LOW LEVEL DIGITAL SPEECH’* The Cambridge Law Journal, July 2012, Vol. 71, No. 2 (July 2012), pp. 355-383

[48] Ibid. 355.

collection, and the use of algorithms to control what users see.[49] The risks and benefits of any self-regulation can only be assessed when the process is fully transparent and fully understood.

In a recent study, the European Parliament's Scientific and Technological Options Assessment (STOA) assessed self-regulation as a policy option.[50] Several benefits were and risks were identified.[51] Firstly, self-regulation has a limited cost. Secondly, companies' responsibilities are increased but without innovation impediment. Thirdly, online platforms are ideally placed to identify problems that warrant regulatory attention and implement solutions**.** Fourthly, they can react quicker and more effectively to these problems when compared to responses to statutorily imposed obligations. For example, using codes of conduct is one option to tackle legal but harmful content which is unsuitable for notice and take down actions.

Self-regulation carries significant risks.[52] Firstly, the commercial objectives of online companies are unlikely to overlap with the objectives of the public service. This may result in outcomes that do not match those of public regulators. Secondly, existing initiatives by online platforms are criticised for lack of effectiveness and seen as lacking the capability to control and manage the online environment unless accompanied by laws on their duties and liability. Thirdly, the frequent absence of clear objectives, and loosely worded pledges and the lack of effective sanctions with any bite is also problematic. This calls into question whether any online platform can independently manage online legal but harmful content and activity such that their responses are compliant with the fundamental rights of users. The concern is that the

[49] S Theil, O Butler, Kate Jones, Harriet Moynihan, Catherine O'Regan, and J Rowbottom. *'Response to the public consultation on the Online Harms White Paper'* Bonavero Institute Report No. 3/2019 1 July 2019 4. Available at https://www.law.ox.ac.uk/sites/files/oxlaw/bonavero_response_online_harms_white_paper_-_3-2019.pdf, last accessed on 17 April 2021.

[50] European Parliamentary Research Service Scientific Foresight Unit (STOA), *'Liability of online platforms'* PE 656.318 February 2021 Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf, last accessed 17 April 2021.

[51] Ibid. 76.

[52] Ibid. 76.

solutions implemented may lead to ‘excessive censorship and activism’.[53]

Overall, given these risks, the complexity of online activity, and the importance of users interests that are at stake, a more refined and clear-cut harmonisation is warranted. “Private policing” is not appropriate as the primary solution for the regulation of online platforms. However, it should be considered to supplement other policy options.[54]

Are there alternative approaches that policymakers should consider?

The issue of online harms has been over a decade in the making. It is a complex issue. Many challenges need to be considered. Given the dynamic nature of online activity, any regulatory framework should have the flexibility to evolve and adapt to reflect this. The policy approach in the White Paper[55] is only one. Other approaches are also potentially available.

One alternative approach to consider is a framework established on human rights.[56] Human rights law already provides the essential basis for a regulatory policy. Such a basis is especially relevant in the online environment where it is critical to balance a range of competing rights and interests in regulatory decision-making. Any proposed regulatory regime would be based on the available human rights law, which in the UK would be the Human Rights Act 1998, the UN Guiding Principles on Business and Human Rights, as well as other international treaties to which it is signed up to.[57] The starting point in adopting this policy approach would be on safeguarding human rights protections. This could be achieved through (i) regulatory codes of practice (such as those proposed) and (ii) regulatory decisions that must be consistent with human rights protections.[58]

[53] Ibid. 76.

[54] Ibid. 76.

[55] Above n 1.

[56] Above n 49, 2.

[57] Above n 49, 3.

[58] Above n 49, 3.

Adopting a regulatory policy consistent with basic standards set out in UK human rights law would provide significant opportunities for policy makers to embed the introduction of 'digital constitutionalism'[59] into the service terms and conditions of in-scope companies. This would represent a significant development in human rights protections and demonstrate leadership on the international stage post Brexit.

CONCLUSION

Tacking online harms is a complex process. The decision to regulate will likely have long lasting consequences in any democratic society. Legislative initiatives are underway in the UK and the EU. Several conclusions can be drawn. Firstly, the UK framework is best described as a "one size fits all" approach. It blurs or wraps illegal and legal but harmful content and activity together into one target. The "one size" strategy is also apparent in a new "general" rather than subject specific statutory duty of care. Secondly, the operation of the statutory duty maybe unworkable ("third party problem") because it gives rise to unique inconsistencies and tensions with existing legal principles. Despite the assumption of online-offline equivalence, it raises the prospect of a two-tier duty system; one version for online harms and the existing one for offline safety. In the any legal challenges that follow, the court will undoubtedly be faced with interpretating the matter regardless of the supremacy of Parliament.

Thirdly, anxieties about the regulatory process and the risks it will be used to suppress or censor lawful online content deemed "harmful" appear justified because of OFCOM's extremely wide discretionary powers. Restrictions or censorship on free expression must meet the ECHR test of proportionality, legality, and necessity in a democratic society. It is unclear how this is satisfied with an unelected regulator deciding what constitutes free speech in the digital environment. The omission of any legal right for an individual to claim damages for duty breaches is significant. It represents a missed opportunity to address the asymmetric relationship between the individual and powerful and well-resourced in-scope companies. Although these companies will be burdened with funding the operation of the regulatory regime, it is very difficult to conclude a fair balance has been achieved for either party.

[59] Above n 17, 27.

Fourthly, compared to state regulation, “private policing” costs less and provides for faster regulatory decision making.[60] However, protecting an individual’s fundamental rights is too important to leave to large companies with commercial objectives. There is a real risk they may be over-zealous and censor legal activity and content to avoid the “regulatory gaze” and sanctions. A more appropriate strategy would include self-regulation as a complimentary approach.[61]

The UK framework will have to function alongside other legislative frameworks relevant to the online environment (data protection and privacy). The UK’s existing human rights framework offers a ready-made alternative policy that needs to be incorporated. The ECHR covers both private and state activities. However, it would have to be developed to authorise enforcement against in-scope companies.

The dynamics of online activity and content is complex. Overall, one cannot conclude that the two major objectives in the framework will be achieved with the framework. Neither can it be said that other jurisdictions would adopt it. What is required is a more comprehensive regulatory approach, one that is perhaps more consistent with the multi-strategy approach envisaged in the EU’s Digital Services Act. This includes illegal and potentially harmful content as well as all digital services that connect consumers to goods and services.[62] Instituting multiple frameworks that strategically target subject-specific harmful activity and content may prove more effective firstly, in preventing the process of ‘disentitlement’[63] of the individual’s fundamental rights, and secondly, in redressing the existing relational asymmetries between the individual and online companies.

[60] Above n 50, 76.

[61] Above n 50, 76.

[62] European Parliamentary Research Service Scientific Foresight Unit (STOA), ‘*Online platforms: Economic and societal effects’* PE 656.336 March 2021. 65 Available at https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656336/EPRS_STU(2021)656336_EN.pdf, last accessed on 7 April 2021.

[63] J E Cohen, ‘*Between truth and power: the legal constructions of informational capitalism’* (2019) New York, NY: Oxford University Press.12.

Bibliography

Baines V, *'Online Harms and Folk Devils: Careful Now'* (24th June 2019) <https://medium.com/@vicbaines/on-online-harms-and-folk-devils-careful-nowf8b63ee25584> last accessed 17th April 2021

Big Brother Watch, *'Big Brother Watch's response to the Online Harms White Paper Consultation'* (12 July 2019) <https://bigbrotherwatch.org.uk/wp-content/uploads/2020/02/Big-Brother-Watch-consultation-response-on-The-Online-Harms-White-Paper-July-2019.pdf> last accessed 17th April 2021

Cohen J E, '*Between truth and power: the legal constructions of informational capitalism'* (Oxford University Press, 2019)

Department for Digital, Culture, Media and Sport, and the Home Office, *'Online Harms White Paper'* 2019, CP 57

Department for Digital, Culture, Media and Sport, and the Home Office, '*Online Harms White Paper: Full Government Response to the consultation'* 2020, CP 354

Dicey AV, *'An Introduction to the Study of the Law of the Constitution*' (8th edition, Macmillan, 1915)

European Parliamentary Research Service Scientific Foresight Unit (STOA), *'Liability of online platforms'* PE 656.318 (February 2021) <https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656318/EPRS_STU(2021)656318_EN.pdf> last accessed 17th April 2021

European Parliamentary Research Service Scientific Foresight Unit (STOA), '*Online platforms: Economic and societal effects'* PE 656.336 (March 2021)

<https://www.europarl.europa.eu/RegData/etudes/STUD/2021/656336/EPRS_STU(2021)656336_EN.pdf> last accessed on 7th April 2021

Mendel T, '*A Guide to the Interpretation and Meaning of Article 10 of the European Convention on Human Rights'* (Council of Europe 2017) <https://rm.coe.int/16806f5bb3> last accessed 17th April 2021

OFCOM, Addressing harmful online content A perspective from broadcasting and on-demand standards regulation (18th Sept 2018) <https://www.ofcom.org.uk/__data/assets/pdf_file/0022/120991/Addressing-harmful-online-content.pdf> last accessed on 17th April 2021

Rowbottom, J *'TO RANT, VENT AND CONVERSE: PROTECTING LOW LEVEL DIGITAL SPEECH'* (2012) The Cambridge Law Journal Vol. 71 No. 2, 3 <https://www.jstor.org/stable/23253650> accessed 30th March 2021

Smith G, '*Online Harms White Paper- Response to consultation'* (28th June 2019) <https://www.cyberleagle.com/2019/06/speech-is-not-tripping-hazard-response.html> accessed on 17th April 2021.

Tambini D, *'The differentiated duty of care: a response to the Online Harms White Paper'* (2019) Journal of Media Law, 11:1, 28 https://doi.org/10.1080/17577632.2019.1666488 accessed 1st April 2021

Theil S and others, *'Response to the public consultation on the Online Harms White Paper'* Bonavero Institute Report No. 3/2019 (1 July 2019) <https://www.law.ox.ac.uk/sites/files/oxlaw/bonavero_response_online_harms_white_paper_-_3-2019.pdf> accessed on 17th April 2021

Woods L, ‘The duty of care in the Online Harms White Paper, (2019) Journal of Media Law, 11:1, 6 < https://doi.org/10.1080/17577632.2019.1668605> accessed on 1st April 2021