**Written evidence submitted by WebGroup Czech Republic, a.s. and NKL Associates s.r.o. (OSB0142)**

## I. INTRODUCTION

1. WebGroup Czech Republic, a.s. (formerly WGCZ s.r.o.) and NKL Associates s.r.o., which specialize in the online hosting of adult content and own the websites xvideos.com and xnxx.com, respectively, (collectively "**WGCZ**" **or** "**we**") welcome the opportunity to submit this written contribution to the Draft Online Safety Bill (Joint Committee) (the "**Committee**") on the UK Government's Draft Online Safety Bill published on 12 May 2021 (the "**Bill**").

2. In the first instance, we are, respectfully, cognisant that it is, on its face, unusual for companies established in the Czech Republic to take an interest in a regulatory development in the UK, given that the UK is no longer part of the European Union and subject to the European *ordre public*. However, as the Committee will appreciate, the borderless nature of the Internet means that this proposed legislation has the potential of having ramifications beyond British borders; indeed, the Bill has the potential of affecting not only WGCZ, but businesses in all corners of the world.

3. WGCZ are operators of online platforms which host adult material, targeting an adult audience. WGCZ fully supports the goals of ensuring the health, safety and well-being of children online, including, among other things, by preventing children's access to any content or product that is addressed to an adult audience. WGCZ underlines that it has never targeted any such audience and does not condone any such access and concurs on the importance of finding effective ways to prevent it. WGCZ has over the years collaborated with authorities all around the globe to join forces in the fight against child sexual exploitation and abuse (**CSEA**) content and to facilitate online child protection. WGCZ is fully cognisant that designing effective and proportionate interventions to protect children from accessing adult content without limiting adult access to the Internet presents a policy conundrum.

4. Our submission is therefore intended, in the spirit of supporting initiatives to prevent minors accessing adult services, to provide the Committee with an appreciation of the impact of this legislation and to invite it to carefully scrutinise the proposed framework. While there is no doubt the Bill's aims of promoting safety online is commendable, it is not without challenges in a globally interconnected system. It is in the interests of both businesses and policy makers that its proposed solutions are effective, balanced, and appropriately accommodate the interests of all parties, including the many users who use and rely on the Internet.

5. We note that the current Bill has expanded its remit to expect providers to be able to manage *any* potential harm that occurs on their platforms. There are some good intentions here – there is no harm in providers demonstrating their risk assessments in

considering how they support the "safety" of users and providing a level of accountability for those less scrupulous providers who do not see the wellbeing of their platform users as their concern. However, as noted in section III below, the concept of the 'duty of care' is amorphous and the Bill fails to set out the extent of a duty of care that providers may have, and what the limits on expectations of protection should be.

6. We take this opportunity to enclose and refer the Committee to our submission of 3 September 2021 to the DCMS Sub-Committee on Online Harms and Disinformation, who are also considering the Bill in parallel with this Committee. This submission is intended to complement our previous comments made to the Sub-Committee. However, for the purposes of this submission, we endeavour to specifically respond to the following questions posed by the Committee in its call for evidence:

   (a) Will the proposed legislation effectively deliver the policy aim of making the UK the safest place to be online?

   (b) Is the "duty of care" approach in the draft Bill effective?

   (c) Does the Bill deliver the intention to focus on systems and processes rather than content, and is this an effective approach for moderating content? What role do you see for e.g. safety by design, algorithmic recommendations, minimum standards, default settings?

## II. WILL THE PROPOSED LEGISLATION EFFECTIVELY DELIVER THE POLICY AIM OF MAKING THE UK THE SAFEST PLACE TO BE ONLINE?

7. As the Committee will appreciate, the nature of the Internet is such that it has an inherent global reach: it can be accessed by users (adults and children) and service providers hailing from all corners of the world.

8. We appreciate that part of the underpinning policy aim of the Bill is to safeguard children, a goal which we also endorse.

9. There are a wide range of businesses which already adopt measures to deter underage access to adult goods and services, ranging from motion picture companies and producers of alcohol or certain video games to gambling online and adult movie sites. Children are as unwelcome on a casino site, an adult gaming site, or an adult movie site, as on a site offering alcohol or tobacco.

10. However, the Committee will undoubtedly recognise that from a technical standpoint, users have the ability to use work-arounds, such as IP proxying or virtual private networks, which allow them to access the Internet notwithstanding barriers that have been put in place by service providers. In this respect, there are inherent limitations of technological solutions, and any legislation seeking to control a global system from a geographically restricted perspective will necessarily be faulty.

11. The United Kingdom is certainly not alone in considering these challenges. States, including France and Germany, as well as the European Commission, are all having similar discussions and grappling with the difficulties associated with such technology. Since a strictly territorial approach will not protect users from online harms sourced from other countries, the UK's coordination with its European allies and neighbours in this space is necessary to achieve the goal of a safer Internet.

12. In light of the above, we respectfully suggest that it may be more accurate to reframe the question posed by the Committee by considering what specific measures would make the UK a place where citizens can expect to be provided with useful and relevant tools to mitigate risk online.

13. To that end, we note that in the 145 pages of the Bill, there are only two mentions of the word "education", found in section 103, which relates to media literacy and the role of the regulator in delivering public awareness programmes.

14. We believe this is a missed opportunity for the Bill to address a crucial aspect of safety online. Public education of online harms should also be a policy priority, with the aim of building the knowledge of users and their resilience to risk. There should be further emphasis on measures integrated in curricula and public education to increase online literacy and warn children of the risks and dangers of operating online, in order to enable them to make rational and informed choices as they navigate the Internet and to adopt appropriate strategies when encountering troublesome content.

## III. IS THE "DUTY OF CARE" APPROACH IN THE DRAFT BILL EFFECTIVE?

15. The Bill's most significant innovation is the establishment of "duties of care" on service providers, which includes duties to address illegal CSEA content. For any such "duties of care" to be effective, service providers subject to such duties should be able to understand the scope of those duties. In particular, they must be able to understand policy makers' expectations and whether the solutions they adopt are sufficient to demonstrate they have discharged their duties under the legislation.

16. As presently drafted, the "duties of care" set out in the Bill are shrouded by a degree of intangibility. Regrettably, the Bill is silent on what constitutes an "effective" versus "ineffective" way of managing the risk of harm, or what would be considered an appropriate or suitable "system or process" to manage such risks.

17. WGCZ would welcome clear guidance as to what these "duties of care" entail. WGCZ, for instance, already adopts a robust system of content control which is aimed at eliminating any content that violates the integrity of minors and at reporting such offences to competent police authorities, as specified in the websites' content control policies.

18. In addition, some of the Bill's language associated with these "duties of care" invite further reflection. For instance, the Bill entrusts service providers with making assessments in relation to "harmful content". The inherent subjectivity and transient nature of "harm" (i.e. the same content may trigger different responses at different times, depending on the user) are likely, absent further clarification, to result in divergent assessments and thus greater regulatory uncertainty. All parties, from service providers to users, stand to benefit from clearer and more precise guidance than that offered in the current draft of the Bill.

## IV. DOES THE BILL DELIVER THE INTENTION TO FOCUS ON SYSTEMS AND PROCESSES RATHER THAN CONTENT, AND IS THIS AN EFFECTIVE APPROACH FOR MODERATING CONTENT? WHAT ROLE DO YOU SEE FOR E.G. SAFETY BY DESIGN, ALGORITHMIC RECOMMENDATIONS, MINIMUM STANDARDS, DEFAULT SETTINGS?

19. We note that all service providers who operate online regularly adopt different systems and processes in the ordinary course of business, and as the question makes reference to different technological solutions, we would reiterate that technology is not a panacea for ensuring safety online. While technology undoubtedly forms part of the online safeguarding toolkit, in our respectful view, the Committee should be cautious about over-reliance of specific technological solutions when it comes to online safety.

20. For instance, algorithms regularly fail to understand context, and artificial intelligence struggles to understand and appreciate nuance when it comes to developments online. Technology also develops at a rapid pace, meaning that systems which exist today may not be fit for purpose or could become obsolete tomorrow.

21. Moreover, specific tools (for instance, age verification technology) may well be unworkable in practice and have unintentional, deleterious effects, and the Committee will be well-aware of the debates surrounding this issue arising out of the Digital Economy Act 2017.

22. Age verification measures vary significantly, each with their own inherent limitations. These include, among others, self-declaration, hard identifiers, digital identities, phone providers checks, facial age estimation, facial recognition, physical verification, and social network content analysis. The plethora of different age assurance tools demonstrates that a one-size all solution is simply not possible and in many respects, deficiencies with the existing methods are ones which technology alone cannot address.

23. Moreover, many civil society organisations, such as the Open Rights Group[1] and UNICEF,[2] as well as the UN Special Rapporteur on the promotion and protection of the right to

---

[1] *See, e.g.,* Open Rights Group, 'ORG Report: BBFC Age Verification Standard is Pointless, Misleading and Potentially Dangerous', 14 June 2019, available at https://www.openrightsgroup.org/press-releases/org-report-bbfc-age-verification-standard-is-pointless-misleading-and-potentially-dangerous/ (last accessed on 16 September 2021 and Open Rights Group, Blog Article: "*The government is acting negligently on privacy and porn AV*", 8 May 2018, available at https://www.openrightsgroup.org/blog/the-government-is-acting-negligently-on-privacy-and-porn-av/ (last accessed on 16 September 2021).

freedom of opinion and expression,[3] have all repeatedly warned about the dangers to privacy and interference with the right to freedom of expression associated with such tools.

24. Many forms of age verification technology involves the gathering of personal information and can involve the amassing of very sensitive personal details, which can lead to its own data protection burdens and dangers. The regime may involve, for example, requesting that a person seeking access to an adult site must divulge to the business operator his personal details, such as identity card or passport numbers, or home address. The business operator will become privy to a mass of potentially sensitive data, as well as being trusted to observe the extensive and prescriptive rules under data protection law and the UK General Data Protection Regulation (UK GDPR). The previously proposed solutions such as the BBFC's Age-verification Certificate involved providers making voluntary and unaccountable promises not to share data with third parties, and many organisations rightly challenged the efficacy of these proposals and their consistency with prevailing rules on data protection and privacy. It is imperative that any legislation acknowledges that registering people's personal details for accessing age-restricted content carries significant risks and challenges.

25. In addition, the imposition of such measures could also result in the unwarranted effect of pushing children towards the dark web, which is far more likely to provide access to illegal content (such as CSEA content). Given the nature of the content in these spaces, they attract many with a sexual interest in children, so driving young people to these spaces could be extremely dangerous for them. There is also the risk of increasing the sharing of pornography through peer to peer channels without the content moderation that is achieved on mainstream pornography channels, where no CSEA is permitted. Finally, these spaces will place young people at greater risk for arrest if they are being monitored.

26. We believe therefore that the Bill's proposal to formally delete the age verification mechanisms introduced by the Digital Economy Act 2017 is warranted, given the clear, demonstrated unworkability of those proposals.

27. Respectfully, members of the Committee without an information technology background might be led to believe that there must exist a technical solution that will straightforwardly resolve the above issues. However, because of the detailed workings of the international software protocols involved in the Internet, nobody has yet been

---

2 *See* UNICEF, Digital Age Assurance Tools and Children's Rights Online across the Globe: Discussion Paper, March 6, 2021, available at https://www.scribd.com/document/511152514/Digital-Age-Assurance-Tools-and-Childrens-Rights-Online-Across-the-Globe (lastly accessed on 16 September 2021).

3 *See* Communication to the Government of the United Kingdom from the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (OL GBR 1/2017), 9 January 2017, available at https://ohchr.org/Documents/Issues/Opinion/Legislation/UK_DigitalEconomyBill_OLGBR1.2017.pdf (last accessed on 16 September 2021).

able to create a technical solution that is able to balance, on one hand, the data protection and civil liberties requirements concerned, and on the other hand, still be functional in an environment where the interchanges involved are international. We reiterate our willingness to participate in any efforts the Committee may wish to pursue in exploring potential solutions.

28. Ultimately, the Bill's focus on systems and processes should necessarily allow organisations to adopt such systems and processes appropriate for their business. The legislation should take care not to unduly burden or penalise organisations who, despite adopting measures to address some of the underlying harms targeted by the Bill, are nonetheless circumvented by determined users or for reasons beyond their control.

## V. CONCLUSION

29. WGZC reiterates its support for initiatives to prevent minors accessing adult services and, in particular, ensuring that well-meaning initiatives do not result in deleterious consequences such as forcing minors onto the dark web and other more dangerous parts of the Internet. We thank the Committee for the opportunity to provide our written observations on the Government's proposals in the Online Safety Bill and welcome the possibility of further engagement with the Committee and its members as the Bill goes through the parliamentary process.

30. As a responsible business, we of course must and do comply with laws and regulations, and in the present case, we urge the Committee to consider the importance of ensuring that the final legislative framework adopted by Parliament and which will become law protects fundamental rights, is not unnecessarily burdensome on the conduct of legitimate business, and provides clarity and predictability for businesses operating via the Internet. It is, respectfully, of paramount importance that the making of the Internet a safer place shall be proportional, effective and avoid impinging on other fundamental freedoms, including the freedom of speech, as well as being mindful of privacy concerns.

**THE INHERENT LIMITATIONS OF TECHNOLOGY**

31. While no one can doubt the policy objective of protecting underage access, the proposal does not address or resolve the core of the challenge: the delicate balance between the importance of the objective and the intrusiveness, in terms of civil liberties, of truly effective measures to prevent underage access.

32. In making this submission, we are mindful of the fact that the Online Safety Bill follows a suite of successes (filtering on public WIFI which in itself is a highly contentious issue), near misses (default filtering on home ISP connections, still only used by a minority of households according to OFCOM[4]), and failures (Part 3 of the Digital Economy Act 2017). As this submission seeks to explain, the reality is that the Bill is not laid on a foundation of success in technology regulation or the use of technology to manage online behaviour.

33. Online services, and the underlying technology that allows them to be implemented, are global by nature. Therefore, geographical boundaries present problems. However, to try to isolate based upon geography is a challenge that introduces extraterritorial jurisdictional issues that are evident within this bill. Geography in an online sense is usually managed through the IP address system, where different countries are assigned different address ranges which, in turn, allows systems to make an approximation of the location of an end user. However, this is not a perfect system and work arounds such as IP proxying and Virtual Private Networks, which are widely used for many privacy enhancing measures, will easily circumvent this. Therefore, any legislation that attempts to control a global system from a geographically restricted perspective is not going to be perfect.

## I. ADDRESSING ONLINE HARMS: THE TANGIBILITY AND PRACTICAL WORKABILITY OF THE "DUTY OF CARE" CONCEPT

34. The Bill's most significant innovation is the establishment of a "duty of care" on service providers, which includes duties to address illegal CSEA content.

35. In that respect, the Bill proposes to impose a number of "duties" on user-to-user service providers. Taking the example of "safety duties", the Bill provides:

> "*(2) A duty, in relation to a service, to take proportionate steps to mitigate and effectively 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—*

[4] https://www.ofcom.org.uk/__data/assets/pdf_file/0025/217825/children-and-parents-media-use-and-attitudes-report-2020-21.pdf

*(a) minimise the presence of priority illegal content;*

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

*(c) minimise the dissemination of priority illegal content;*

*(d) 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*[5]

36. The Bill also specifies that:

> *(6) In determining whether a step, system or process is proportionate for the purposes of this section, the following must be taken into account—*
>
> *(a) all the findings of the most recent illegal content risk assessment (including as to levels of risk and as to nature, and severity, of potential harm to individuals), and*
>
> *(b) the size and capacity of the provider of a service.*[6]

37. As presently drafted, the duties introduced by the Bill are amorphous: it is difficult to assess what might be considered to be an "effective" versus "ineffective" way to manage the risks of harm to individuals, for example, or to understand what "systems or process" would be considered appropriate.

38. WGCZ would welcome clear guidance as to what the 'duty of care' entails. WGCZ, for instance, already adopts a robust system of content control which is aimed at eliminating any content that violates the integrity of minors and the reporting of such offences to competent police authorities, as specified in the websites' content control policies.

## II. THE DIFFICULTIES WITH PREVIOUS AGE VERIFICATION PROPOSALS

39. One of the possible "system or process" that have been previously considered is an "age verification mechanism", which this Committee will be familiar with as part of its past consideration of the Digital Economy Act.

40. The Committee will recall that during the consideration of the Digital Economy Act, the United Nations Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression wrote an open letter to the British government expressing his concerns about a number of the proposals:

---

[5] Clause 9(2) and 9(3) of the Bill

[6] Clause 9(6) of the Bill

"*First, I am concerned that the age verification provisions **give the government access to information about citizens' viewing habits and data***. [...] *In addition, the age verification requirement can easily be abused, such as **hacking**, **blackmail** and other potential credit card **fraud***. [...]

*I am concerned about the lack of **privacy** obligations in the bill, when it effectively provides for the use of technologies that limit privacy rights through the requirement of age verification.* [...]

*In addition, I am concerned about the lack of **judicial review** of the age verification regulator's authority to shut down websites that do not comply with the age verification requirement...*"[7] (emphasis added).

41. The Government's appointment of the British Board of Film Classification as the intended age verification regulator and its attempts to propose an 'age verification certificate standard' was also widely criticized by organisations such as the Open Rights Group, who wrote that the standard was "*pointless, misleading and potentially dangerous."*[8]

42. The Committee will also be cognisant that from a technical standpoint, any such age verification mechanisms could only apply within the UK, allowing users to access adult sites via VPNs or IP proxying, by simulating access from another jurisdiction where it would not be restricted.

43. Moreover, the imposition of such measures could also result in the unwarranted effect of pushing children towards the dark web, which is far more likely to provide access to illegal content (such as CSEA content). Given the nature of the content in these spaces, they attract many with a sexual interest in children, so driving young people to these spaces could be extremely dangerous for them. There is also the risk of increasing the sharing of pornography through peer to peer channels without the content moderation that is achieved on mainstream pornography channels, where no CSEA is permitted. Finally, these spaces will place young people at greater risk for arrest if they are being monitored.

44. Without a uniform, consistent, and free, age ID scheme, a technical solution will always struggle. So a provider might implement an age verification solution that uses a number of different measures (for example, the NSPCC/IWF Report/Remove service[9] uses passport, driving licence or YOTI) but these will not be effective for all young people. To

---

[7] Communication to the Government of the United Kingdom from the UN Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression (OL GBR 1/2017), 9 January 2017.

[8] Open Rights Group, 'ORG Report: BBFC Age Verification Standard is Pointless, Misleading and Potentially Dangerous', 14 June 2019, accessed at: https://www.openrightsgroup.org/press-releases/org-report-bbfc-age-verification-standard-is-pointless-misleading-and-potentially-dangerous/

[9] https://www.childline.org.uk/info-advice/bullying-abuse-safety/online-mobile-safety/remove-nude-image-shared-online/

continue with the NSPCC/IWF service as an example, all of the AV measures used on that system have an associated cost. This will mean that many young people will not be able to afford to verify their age, and will not be able to use it.

45. It would seem unfair and unrealistic to expect companies to invest in risk assessment and subsequent software tools to implement risk mitigation measures, just to be told they will still be fined as they failed in their duty of care to let in a determined, duplicitous young person who decides to bypass age verification measures with either their parent's login or a Virtual Private Network.

46. We believe therefore that the Bill's proposal to formally delete the age verification mechanisms introduced by the Digital Economy Act 2017 is warranted, given the clear, demonstrated unworkability of those proposals.

47. If the Government is serious in its view the age verification has to be part of the online safeguarding toolkit, and placing expectations on companies to implement a foolproof system, they should propose the underpinning infrastructure, which is a national ID card scheme, and weigh all of the privacy concerns and debates that brings from the public.

## III. PUBLIC AWARENESS AND EDUCATION ON ONLINE SAFETY

48. The Bill will not succeed without a parallel emphasis on developing public discourse and educating the public about safety online.

49. Children are increasingly adept at using new technologies and navigating the Internet. Parents must play the most crucial role in ensuring their children are adequately protected at home, for instance, using built-in and other widely available (and free) controls on content or filtering.

50. Measures should also be integrated in curricula and public education to increase online literacy and warn children of the risks and dangers of operating online, thereby enabling them to make rational and informed choices as they navigate the Internet and to adopt appropriate strategies when encountering troublesome content.

## IV. CONCLUSION

51. WGZC reiterates its support for initiatives to prevent minors accessing adult services and, in particular, ensuring that well-meaning initiatives do not result in deleterious consequences such as forcing minors onto the dark web and other more dangerous parts of the internet. We thank the Committee for the opportunity to provide our written observations on the Government's proposals in the Online Safety Bill and welcome the possibility of further engagement with the Committee and its members as the Bill goes through the parliamentary process.

52. As a responsible business, we must and do comply with laws and regulations, and in the present case, we respectfully ask the Committee to consider the importance of ensuring

that the final legislative framework adopted by Parliament and which will become law protects fundamental rights, including the most cherished rights of privacy and free expression, is not unnecessarily burdensome on the conduct of legitimate business, and provides clarity and predictability for businesses operating via the Internet.

*27 September 2021*