Written evidence submitted by Cloudflare (OSB0091)

Cloudflare appreciates the opportunity to provide comments to the Joint pre-legislative scrutiny Committee on the Draft Online Safety Bill. We have focused our response on only a few areas outlined by the Committee; we specifically discuss the scope of the draft Bill, as well as exemptions, definitions and enforcement mechanisms (e.g. "access restriction orders").

Introduction to Cloudflare

Cloudflare provides security, reliability, and performance services to a significant portion of the Internet, with approximately 19% of Fortune 1000 companies using our service. In support of its mission to "help build a better Internet," Cloudflare believes in making cybersecurity services easily accessible, offering both free and paid services that users can sign up for online. The broad availability of Cloudflare's services helps mitigate the risk posed by malicious cyber activities and improves the reliability and performance of the Internet for everyone online. In addition to making sure security and reliability services are widely available to everyone who wants to or needs to operate online, Cloudflare has undertaken particular efforts to ensure that a variety of important but underfunded organizations are protected from cyberattack, including civil society and independent journalism organizations,[1] election infrastructure,[2] and political campaigns.[3] With a growing network of 250+ data centers globally, Cloudflare plays an increasingly important role in developing, improving and investing in the underlying infrastructure of the Internet for the benefit of all.

Cloudflare's business has never been about analysing the content that flows over its network but has focused on securing and optimizing the process used to get that content to where it needs to go. As such, Cloudflare's services facilitate the businesses of other providers, such as those at the application and content layer of the Internet stack. Cloudflare provides a global Content Delivery Network (CDN) service with unique performance optimization capabilities: we cache content for a short, temporary period and we optimize outbound content for the benefit of local users. Cloudflare's core services also include both internal network facing and Internet facing security services, such as zero trust services, a web application firewall, protection from distributed denial of service and other attacks, and Domain Name System (DNS) services.

---

[1] https://www.cloudflare.com/galileo/

[2] https://www.cloudflare.com/athenian/

[3] https://www.cloudflare.com/campaigns/

Scope

One of the questions posed by the PLS Committee relates to the types of services that are considered in scope of the draft Bill. Understanding that the goal of the draft legislation is to devise a regulatory framework that can most effectively address the issue of illegal and harmful content online, we see an important distinction between services that curate content - such as social media platforms and search engines - and Internet infrastructure services which simply help to move the traffic bits securely and efficiently. This technical layer of the Internet stack is substantially different to the content layer which is inhabited by companies that allow users to share or discover user-generated content or to interact with each other online (e.g. social media platforms, file hosting sites, public discussion forums, messaging services, search engines).

We therefore believe that the draft Bill has provided the appropriate regulatory focus in this respect, taking a risk-based and proportionate approach as suggested already in the DCMS Online Harms White Paper in 2019, and the Government's response to the public consultation in 2020. The intended scope of the Draft Bill ("user-to-user-services" & search engines) seems a proportionate one, focusing on those services which are closest to the content at hand, and that can also take the most effective and proportionate action against such (illegal or harmful) content online. Nonetheless, it is critical to ensure that the guidelines of the intended regime are clear, so businesses of all sizes understand what they will be required to do and have enough time to prepare for implementation. This is particularly important to ensure that small businesses are not overburdened with compliance requirements.

Exemptions & definitions

Although Cloudflare is supportive of the intended targeted scope of the draft Bill focusing on content curation services, we would recommend that legislators provide a more explicit mention of the exclusion from the draft Bill's safety duties of both enterprise and business (software) services (B2B), as well as other types of "access facilities" that are mentioned in the Explanatory Notes[4], such as ISPs, CDNs, domain name services, and web hosting companies.

While it seems clear from the guidance in the explanatory notes[5] that those types of services are not being considered in scope of the law, the actual legislation unfortunately is not as explicit. The guidance itself is not law, and more specific provisions in the Draft Bill would give

[4]https:/assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/985031/Explanatory_Notes_Accessible.pdf - point 729, page 100

[5]Part 7, page 100

much needed legal certainty for the services which are (rightly) intended to be out of scope of the safety/duty of care obligations. The most effective way of ensuring that the Government's clearly established intentions are met would be through the finding of a clearer formulation regarding exemptions.

Access restriction orders

The draft Online Safety Bill contains provisions which would allow Ofcom to request a court to produce "access restriction orders" for the above mentioned "access facilities". Moreover, other business disruption measures are proposed, such as service restriction orders for ancillary services such as advertising or payment providers. Practices such as business disruption and access restriction (for example based on ISP blocking) are blunt enforcement tools which do not fit well with the cooperative environment that will be required of all stakeholders to address this complex and new area of regulation. In our view, the proposed business disruption measures should therefore only be used as a measure of last resort, in case all other enforcement options have been exhausted, and its use should be carefully considered by Ofcom.

Considering the intended scope of services which could be seen as "access facilities" according to the guidance, Ofcom should take into consideration the proportionality and effectiveness of measures that different service providers can take in terms of "preventing, restricting or deterring individuals in the UK from accessing [a] service"[6]. For example, as regards ISP blocking, there is a broad consensus, as noted by OFCOM in 2014[7], that all filtering solutions face risks of circumvention by a dedicated and technically competent user and as supported by a range of advice available online. The Internet Society[8] has also looked at this area, concluding that using Internet blocking to address illegal content or activities is "generally inefficient, often ineffective and generally causes unintended damages to Internet users". Overall, this is an outdated enforcement tool that should be retired.

Generally, the examples given in the Explanatory Notes of services that would be considered an "access facility" (in addition to ISPs and app stores) and which could face an access restriction order, may not fully correspond with the description of such facilities in the actual legislation[9]. For example, Content Delivery Network services cannot "impede access" of a user to a website

---

[6] See: Explanatory notes, point 603 page 82

[7] Page 22 https://www.ofcom.org.uk/__data/assets/pdf_file/0019/27172/Internet-safety-measures-second-report.pdf

[8] https://www.internetsociety.org/resources/doc/2017/internet-content-blocking/

[9] Part 93 subsection 10 of the Draft Bill: "For the purposes of this section, a facility is an "access facility" in relation to a regulated service if the person who provides the facility is able to withdraw, adapt or manipulate it in such a way as to impede access (by means of that facility) to the regulated service (or to part of it) by United Kingdom users of that service."

or application. We are in this respect also concerned to see “security software” on this list, as it implies that a way Ofcom could seek to prevent or block access of users to a regulated service would be to remove its security protections and make it vulnerable to cyberattack. This seems a misguided approach and not proportionate to the purpose of the enforcement measures.

16 September 2021