Your response

Volume 6: Information gathering and enforcement powers, and approach to supervision.

Information powers

Question 52:	
i)	Do you have any comments on our proposed approach to information gathering powers under the Online Safety Act?
Response:	
ii)	Please provide the underlying arguments and evidence that support your views.
Response:	
iii)	Is this response confidential? (if yes, please specify which part(s) are confidential)
Response:	

Enforcement powers

Question 53:	
i)	Do you have any comments on our draft Online Safety Enforcement Guidance?
Response: YES - see response to ii)	
ii)	Please provide the underlying arguments and evidence that support your views.
Response: This response focuses on Volume 6 and Annex 11 of the consultation, and specifically on the processes and governance for (interim) access restriction orders, covering the following points:	

1. Overall approach to access restriction orders, technical feasibility and financial implications for access facilities; and
2. Changes to internet architecture and implications for blocking orders.

While we do not cover this in more detail below, we would also welcome greater clarity around how Ofcom intends to work with organisations from across the ecosystem that provide input in the blocking and filtering of content, e.g. the IWF.

Overall approach to access restriction orders, technical feasibility and financial implications for access facilities

The guidance foresees regular, but not mandatory engagement with access facilities prior to Ofcom applying for an access restriction order. While we understand Ofcom's reservation about mandatory

consultation requirements, we urge Ofcom to set out in more detail under what circumstances they would not consult with an access facility. Even just within our membership, there is a wide range of business sizes with significant differences in capability to comply with access restrictions orders, and we believe that it is important to prioritise engagement to avoid undue implications.

The draft guidance suggests in A9.20 that Ofcom can ask access facilities to effectively implement an access restriction order voluntarily. This is not explicitly envisioned by the OSA and we urge Ofcom to set out more clearly under what circumstances and with what safeguards it would go down the voluntary route.

More broadly, we would encourage Ofcom to undertake an assessment of the number of access restrictions orders that it expects to apply for. While we understand that access restrictions orders are seen as a measure of last resort, the number of regulated services has increased significantly during the passage of the OSA, which has also increased the likelihood that Ofcom will need to apply to an access restriction order.

We would also welcome further engagement with Ofcom around the actual *on-the-ground* implementation of access restriction orders. While we understand that some of this will be left to the discretion of the courts, it is still important to ensure a process that provides sufficient notice and time for access facilities to engage with, respond to, and implement a court order.

We would further welcome more detail on what type of blocking or filtering technologies Ofcom envisions to be used, whether Ofcom will specify minimum standards, e.g. around effectiveness, and to what degree Ofcom will take into account the capabilities of access facilities.

Another area where more clarity would be appreciated is the process for reinstatement of access to content if the site owner agrees to make changes to bring them into compliance with the OSA.

With the above in mind, we would welcome more information from Ofcom on:
   A. Number of Access Restriction Orders Ofcom expects to issue, especially in the context of commercial pornography being included.
   B. When Ofcom expects to start the regime and whether they plan to ramp it up or start at high capacity?
   C. Details about the consultation process and under what circumstances they would not consult with an access facility.
   D. Details about when Ofcom would seek voluntary compliance with access restrictions orders.
   E. Details about *on-the-ground* compliance, including timeframes and notices periods.
   F. Details about blocking/filtering technology and minimum standards.
   G. Details about the reinstatement process for content.

Changes to internet architecture and implications for blocking/filtering orders

The Internet, and the architecture it relies on, are constantly evolving. Of particular relevance to the application of access restriction orders are the emergence of new forms of encryption such as DNS over HTTPS (DoH) which is being rolled out by Mozilla (Firefox) and Google (via Chrome), Private Relay which Apple has enabled for a large part of its user base, as well as the emergence of VPNs as consumer (rather than enterprise) product.

Crucially, the level of consumer input to enable these technologies ranges from zero (e.g. in relation to Apple Private Relay or DoH that is enabled within browsers or applications) to minimal (e.g. in relation VPNs). These developments have had a significant impact on how internet traffic is handled, and it has essentially led to dilution of the gatekeeper role that historically used to be performed by local access providers which have traditionally been the target of blocking and filtering orders.

While the Online Safety Act recognises these developments through the broad concept of access facilities, it is largely silent about the complex interplay between different services and how these should be handled. For example, an access restriction order that only applies to a local ISPs is unlikely to be effective for users, including children, that use an Apple device where Private Relay is enabled, or that use a browser where DoH is enabled, or a device where a VPNs is active.

Two core considerations flow from this:
1. **Effectiveness:** In order to be effective, an Access Restriction Order would need to cover all services that are likely to play a role in the facilitation of access.
2. **Proportionality:** An Access Restriction Order that fails to meet the first consideration, is unlikely to be proportionate if it imposes significant cost and administrative burdens on individual services that would effectively be asked to implement an ineffective order.

With the above in mind, we would welcome more information from Ofcom on:
A. Whether Ofcom will formally set out what type of players are considered access facilities.
B. Whether Ofcom will put in place a formal mechanism for identifying the most relevant access facilities for a specific access restriction order.
C. Whether Ofcom will address the different players in the stack at the same time, or subsequently, e.g. ISPs, CDN, hosting.
D. Whether Ofcom will take into account, size, technical capability and related factors when selecting access facilities.

Conclusion

We would welcome further engagement with Ofcom around the implementation of access restriction orders to ensure that they operate effectively and proportionately in a highly complex online environment.

iii) Is this response confidential? (if yes, please specify which part(s) are confidential)
Response: NO