11 October 2022

EDRi briefing note on Council amendments for Article 16-18

Council document 12354/22 contains a number of very problematic amendments for blocking orders (Articles 16-18). Unlike in the Commission's text, the Council propose that blocking orders can be used for content hosted in the EU, despite the fact that removal orders should be possible (and used instead). Furthermore, the Council propose that the order can cover unknown CSA material, which will effectively require Internet Access Service (IAS) providers to monitor internet traffic of all users. Furthermore, almost all safeguards in the EC proposal are removed or watered down.

Extended scope of blocking orders
In the EC proposal, blocking orders can only be issued for known CSAM, represented by a list of URLs. With the Council amendments, blocking orders can be issued for known as well as unknown CSAM. In both cases, the IAS provider must take reasonable measures to prevent users from accessing the material subject to a blocking order.

The Council document does not contain any recitals, so it is very unclear what "reasonable measures" means in the context of unknown CSAM. IAS providers are not allowed to monitor the internet traffic of their users since there is no legal basis in the ePrivacy Directive (ePD) for such processing of communications data. Unlike detections orders (Article 7), the blocking order provision in Article 16 does not derogate from the ePD. If blocking unknown CSAM is to be interpreted similar to a detection order (Article 7), the measure will require some traffic analysis for which the provider has no legal basis. Furthermore, with encrypted internet traffic (e.g. HTTPS to access websites), the IAS provider is technically prevented from doing any traffic analysis of both content and URLs accessed (see below).

Alternatively, "reasonable measures" could perhaps mean that the IAS provider must assess the content hosted on all possible websites on the internet which could be accessed by its users, and proactively block those websites or URLs which contain CSAM. However, this would be an impossible task.

No requirement that the illegal CSAM is hosted outside the EU
In the EC proposal, blocking orders can only be used for content hosted outside the EU (by service providers that are outside the jurisdiction of removal orders in Article 14), and only if the hosting service provider refuses to (voluntarily) remove the content (Article 36(1), point b).

The Council amendments remove these conditions set out in Article 16(2)(a), which means that blocking orders can be used in cases where removal is possible. Since blocking orders generally require less effort than removal orders, there is a clear risk that blocking orders will be favoured by national competent authorities. This will significantly weaken the fight against dissemination of CSAM because removal of the illegal content where it is hosted is the only effective way to prevent access. A blocking order does not prevent access from domestic IAS providers which are not listed in the order or from IAS providers in other Member States. Furthermore, blocking access to internet content is generally ineffective since the blocking can be circumvented in various ways.

Removing the content at source (where it is hosted) also ensures that the measure is targeted to the specific illegal content, without adversely affecting legal content. This is often not possible for

blocking orders, especially if HTTPS (encryption) is used, because this makes URL blocking technologically impossible (see below).

Blocking orders can be issued directly by police authorities
The Council amendments allow blocking orders to be issued by a national competent authority, which can be a police authority. This removes the important safeguard in the EC proposal of prior authorisation by a judicial authority or an independent administrative authority.

If the competent authority is not the Coordinating Authority, which must be an independent administrative authority, the Coordinating Authority can oppose the order (recommend withdrawal) if the order manifestly infringes the CSA Regulation or fundamental rights. This is the same weak (and inadequate) safeguard as for cross-border removal orders in Article 4 of the Terrorist Content Online Regulation.

With the absence of prior independent review by a court or independent administrative authority, the Council text is unlikely to comply with Member States' obligations under the European Convention of Human Rights, as interpreted by the European Court of Human Rights in its judgments on internet blocking.

No effective time limitation for blocking order
The Council amendments remove the requirement that blocking orders must apply for a maximum period of five years (which can, of course, be renewed with a new order if CSAM is still disseminated from the website). In practice, orders will apply indefinitely, and the only safeguard in the Council text is a rather weak requirement for the Coordinating Authority to assess at least once a year whether there are substantial changes to the grounds for issuing the blocking order.

Removal of other important safeguards
The Council text proposes weaker grounds for issuing a blocking order. There is no requirement to seek removal of the content first, as discussed above. The requirement for the competent authority to assess and provide evidence that the CSAM is actually accessed from the network of the IAS providers under consideration for a blocking order (Article 16(4), point a) is deleted.

The proportionality assessment in point d of Article 16(4) is also deleted. Blocking orders can be issued without a requirement of striking a fair balance between the fundamental rights of all parties affected, including those of users (freedom of expression and access to information) and IAS providers (freedom to conduct a business). This is unlikely to comply with CJEU jurisprudence on internet blocking, in particular C-314/12 - UPC Telekabel Wien.

URL blocking and encryption
Nota bene*: the comments below apply to the EC proposal as well as the Council text.*

Blocking at the URL level has the notable advantage of ensuring that the blocking orders can be targeted to specific material which has been identified by competent authorities as illegal (CSAM). This can significantly reduce, and in principle eliminate, the risk of over-blocking (i.e. blocking legal content).

The challenge, however, is the implementation of the blocking order, as this requires that the IAS provider has technical means of inspecting the URLs accessed through the internet connection. Otherwise, the URLs with illegal material cannot be blocked. Such inspection is technically

possible with HTTP through Deep Packet Inspection (DPI), which is used in the Cleanfeed content blocking system operated by IAS providers in the UK on a voluntary basis.

However, today almost all internet traffic is encrypted when transmitted between the end-user requesting it and the server delivering it (HTTPS for web traffic). For HTTPS and other encrypted internet traffic, it will not be technically possible for the IAS provider to execute blocking orders at the URL level. Unlike providers of interpersonal communications services, IAS providers cannot deploy detection technologies at the device level of end-users (similar to Client-Side Scanning) since internet access does not take place through a specific application controlled by the IAS provider.[1] In short, there is no possible way for the IAS provider to break or circumvent encryption because the encryption is not controlled by the IAS provider that simply transmits internet packets, whether encrypted or not.

With the pervasive use of transport-layer encryption (e.g. HTTPS), a blocking provision for URLs will have very limited value for competent authorities due to the general technical impossibility of IAS providers implementing it. With HTTPS, it is only possible to block access to illegal content at the website (domain) level, which immediately raises the issue of over-blocking, since the order effectively covers all URLs, present and future, pointing to that website. It is highly unclear whether the blocking measure in Articles 16-18 can be used at the domain/website level because this requires a proportionality assessment not foreseen by Articles 16-18, where the blocking order is targeted to specific CSA material identified as illegal. Blocking at the domain level will affect illegal as well as legal content at the hosted website, which in many cases will constitute a disproportionate interference with freedom of expression and access to information.[2]

1 If the IAS provider deploys a man-in-the-middle attack on HTTPS traffic in order to inspect the URLs accessed and block certain URLs, the connection to the website will be rejected (with a certificate warning) by the user's browser because the IAS provider cannot present a valid certificate for the domain name. Public campaigns to combat online fraud and promote good cybersecurity practices advise users never to ignore these certificate warnings and proceed to the insecure website. Web browsers also make it increasingly hard for users to proceed to a website with a certificate warning. For these reasons, we consider it technologically impossible for IAS providers to block URLs when HTTPS is used because any attempt to do so would literally break (destroy) security on the entire internet.

2 In 2008, the Internet Watch Foundation (IWF) in the UK put an image from a Wikipedia article on its URL blocking list, see https://en.wikipedia.org/wiki/Internet_Watch_Foundation_and_Wikipedia. The content was legal in the US where Wikipedia is hosted. With HTTP access, it is technically possible to block access to a single image on Wikipedia, but the fine-grained blocking will not work for HTTPS. If faced with a similar situation in 2022, where all Wikipedia access is based on HTTPS, the IWF would undoubtedly refrain from blocking such content on Wikipedia because this would entail blocking access to the entire online encyclopedia, which is clearly disproportionate.