Council of the European Union
General Secretariat

Interinstitutional files:
2020/0361 (COD)

Brussels, 15 September 2021

WK 10800/2021 INIT

LIMITE

COMPET	**PI**
MI	**AUDIO**
JAI	**CONSOM**
TELECOM	**CODEC**
CT	**JUSTCIV**

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

MEETING DOCUMENT

From:	NL Delegation
To:	Delegations
Subject:	Digital Services Act: NL proposal: Addressing the issue of abuse of hosting for manifestly criminal offences

Digital Services Act (DSA)
Addressing the issue of abuse of hosting for manifestly criminal offences

Problem definition: The abuse of hosting services for criminal activity
Criminal activity online is an escalating challenge. This growth was already apparent before the COVID pandemic spurred business and civil activities to migrate online, and the growth has accelerated ever since. Many types of serious crime perpetrated online, such as the dissemination of malware (including ransomware) and Child Sexual Abuse Material (CSAM), types of fraud and the trading of illegal goods such as weapons and drugs, need hosting services to achieve the scale we see today. The services of hosting providers are therefore being abused for many types of serious crime.

Many hosting providers take measures against the abuse of their services for such illegal activities. Unfortunately, there are also hosting providers who do not take sufficient, or even basic measures. This gives criminals the opportunities they need to conduct their actions, resulting in more crime and more victims online, and greater challenges for law enforcement. An obligation to take adequate measures, depending on the specific business, services and risks, would help mitigate the risk of abuse and reduce serious crime and the number of victims on the internet, while creating a level playing field for those hosting providers that already act responsibly.

For online platforms, the exemption of liability puts a premium on not having actual knowledge of illegal content. Notice-and-take-action mechanism to counter this have proved insufficient. The current DSA proposal does not provide for possibilities to hold online platforms to account for making public and disseminating illegal content. Many online platforms, especially those that are very large, already have systems in place to counter illegal content. However, manifestly illegal content is, after being noticed on very large platforms, often moved to alternative, smaller platforms that have less sophisticated means to counter it, moving the risk from large to smaller platforms.

The proposal below aims to address these risks. It has a similar setup as Articles 26 and 27 of the current DSA proposal: it requires hosting providers to assess risks and take measures accordingly. Its applicability does not depend on the size of the hosting provider. Small hosting providers are not less vulnerable to abuse than larger ones. Therefore, measures to be taken should depend primarily on assessed risks.

Importantly, general content monitoring should not be required and hosting providers should fully respect fundamental rights, in particular the right to freedom of speech. The specific type of measure could be left to the hosting provider. Ideally, measures chosen are regarded as (existing) best practices in the hosting sector. Because of the dynamic nature of the market, what is considered as best available measures may change over time. Therefore, the proposal allows for flexibility for developments in the sector, making it future proof.

The proposal should not be understood as necessarily and immediately leading to a much higher degree of content moderation throughout. Instead, it should be understood as a way to force certain hosting service providers to catch up. It is primarily targeted at mala fide hosting service providers and providers that are lagging behind significantly. It prevents content providers from migrating to another hosting service provider in order to more easily disseminate illegal content.

To ensure compliance by all hosting providers that provide services in the Union, Articles 41 and 42 DSA would give the Digital Service Coordinator the power to enforce these obligations, including the power to impose proportionate remedies where the measures of the service provider are deemed insufficient. Finally, to avoid fragmentation of the internal market and ensure uniform application of these obligations, the European Commission, in conjunction with the Board (OR: and/or) could be empowered to issue interpretative guidelines.

Text proposal Chapter III, section 2
Art. 15b
1. Services providers shall identify, analyse and assess at least once a year any significant risk for the misuse of their services for manifestly criminal offences stemming from the functioning and use made of their services in the Union.
2. Without prejudice to article 7 service providers shall put in place reasonable, proportionate, effective and non-discriminatory mitigation measures to address the risk and, if any, actual misuse of their services for manifestly criminal offences.

3. The decision as to the choice of these measures shall remain with the service provider with due regard to their size and level of risk of misuse for manifestly criminal offences. Such measures may include:

a) an acceptable use policy regarding what is expected of the recipients of the services in case of manifestly criminal offences, and to suspend the services to, and/or end the contractual relationship with the recipient of the services who regularly or consistently does not act upon manifestly criminal offences

b) immediate measures to prevent further harm when knowledge of manifestly criminal offences is obtained and the continuation of those manifestly criminal offences may result in serious harm. Examples of such offences are the dissemination of CSAM, malware (including ransomware) and phishing emails, and the hosting of malicious or fraudulent webshops.

c) to ensure correct and up to date customer details, for (but not only) direct contact in case of manifestly criminal offences

d) proactive engagement with recipients of services in case of manifestly criminal offences or vulnerabilities in hardware or software that can be abused for such offences

e) industry best practices to prevent and address manifestly criminal offences

f) adequate measures that can reasonably be expected to obtain information on vulnerabilities or manifestly criminal offences regarding their networks and services, for example by connecting to available information sources

g) adequate measures that can reasonably be expected to diminish the effects of manifestly criminal offences on their networks for other users in general