[redacted]

s 22(1)(a)(ii)

s 22(1)(a)(ii)

Title: s 33(a)(iii)
MRN: s 22(1)(a)(ii) 30/09/2025 s 22(1)(a)(ii)
To: Canberra
Cc: RR : Indo-Pacific Posts, Europe Posts
From: Brussels
From File:
EDRMS Files:
References: s 22(1)(a)(ii)
Response: **Routine, Information Only**

Annotations: s 33(a)(iii)
Summary

s 33(a)(iii)

According to the Internet Watch Foundation, the EU is at the epicentre of hosting online child sexual abuse, with three in every five child sexual abuse reports globally (59 per cent) hosted in an EU member state. In 2023 alone, there were some 1.3 million reports of child sexual abuse in the EU. The Netherlands is said to host more online child sexual abuse content than anywhere else in the world. s 33(a)(iii)

As current president, Denmark has identified tackling child sexual abuse material as a priority.

Existing protections

2. A crucial tool for identifying child sexual abuse material in the EU has been a temporary rule dating from 2021 allowing platforms to scan for content containing child sexual abuse material and report this material voluntarily. Entities are provided with a temporary exemption from strict EU privacy laws. Originally set to expire in 2024, this measure has now been extended to April 2026. By comparison, in the US it is mandatory for platforms to report any instances of child sexual abuse found on networks to the US National Center for Missing and Exploited Children. The EU acknowledges it currently relies heavily on US authorities for reports of online child sexual abuse occurring in the EU.

3. Another critical tool protecting children online in the EU is the Digital Services Act, or DSA (in force from February 2024), which was landmark legislation in efforts to regulate the digital realm. In July, the EU published new guidelines on the protection of minors online

[redacted]

[redacted]

s 22(1)(a)(ii)

s 22(1)(a)(ii)

under the DSA, applicable to all online platforms accessible to minors.

4. The EU also has a Directive on combating the sexual abuse and sexual exploitation of children, intended to harmonise criminal legislation of EU member states. The Directive is being updated in light of technological developments, including AI-generated child sexual abuse material (the UK became the first country to legislate against AI sexual abuse offences in February). Even in cases when the content is fully artificial, the concern is that such material contributes further to the exploitation of children. In February, Europol (under Ope ration Cumberland) supported national authorities in the arrest of 25 individuals involved in a criminal group distributing material fully generated by AI. [**Comment**: The Australian Federal Police are delivering a Regional Cyber Crime Training Program in Budapest in October, providing an opportunity to further deepen cooperation in the fight against child exploitation material].

What more can be done?

5. A new regulation on preventing and combating child sexual abuse online is currently undergoing EU legislative processes. The Regulation to Prevent and Combat Child Sexual Abuse has been under consideration by EU institutions since May 2022, with the next key vote on the proposal expected mid-October. In its current form, the proposal seeks to establish permanent obligations for service providers to detect, report, and remove child sexual abuse material. The proposal also provides a legislative basis for the establishment of a European centre to prevent and counter child sexual abuse (similar to the US).

s 33(a)(iii)

Other member states like Spain have previously supported allowing specific channels into encryption services in certain circumstances and recently the Spanish parliament passed some of Europe's most comprehensive online child protection legislation. In July, Austria passed a national law allowing intelligence services to temporarily intercept encrypted and unencrypted messages (including on services like WhatsApp and Signal) in certain circumstances where there is deemed to be a risk of terrorist activity, espionage, or child exploitation. Slovenia does not have a law granting backdoor access but does have legislation allowing for the criminalisation of encryption if used for the concealment of illegal activities. Similarly, Hungary only requires encrypted service providers to grant access to intelligence agencies upon request.

[redacted]

[redacted]

s 22(1)(a)(ii)

s 22(1)(a)(ii)

Comment

s 33(a)(iii)

text ends

Sent by: s 22(1)(a)(ii)
Prepared by:
Approved by:
Topics: INTERNATIONAL SECURITY/Cyber Policy, INTERNATIONAL SECURITY/Law Enforcement, POLITICAL-ECONOMIC/International Political, SOCIAL ISSUES/General

▼New Distribution

s 22(1)(a)(ii)

