

European Union Terrorist Content Online Transparency Report

February 29, 2024

The following report is published in accordance with Articles 7(2) and 7(3) of EU Regulation 2021/784, addressing the dissemination of terrorist content online. This report contains information for a period of three months and seventeen days, from 13 September 2023 (the day WhatsApp Channels was launched in the EU) to 31 December 2023.

1. GENERAL OBSERVATIONS

General observations outlining the efforts undertaken by WhatsApp to eliminate content violating our Terms and Conditions on our platform.

WhatsApp Ireland Limited, which provides WhatsApp Channels ("Channels") for users in the EU, aims to be the most private broadcast service available. Channels is a one-to-many broadcast service, separate from private messaging, designed to help people follow information from people and organizations that are important to them. In order to comply with legal and sanctions obligations, we developed Whatsapp Channels Guidelines which state that we do not allow people to share content that constitutes a credible threat to public or personal safety, incitement of violence, organization or coordination of violent or criminal activities.

WhatsApp detects and removes violating content by using a combination of automated data processing, human review and user reports.

WhatsApp enables users to report any channel or specific update within a channel. We provide clear information on how to report a channel, and users can report problematic content by



reporting either the channel or the specific channel update. Users can report a channel or update from directly within the channel using simple reporting tools.

We allow individuals and their authorized representatives in the European Union to report content that they believe violates local laws. This includes an <u>intake channel</u> to report content, if users believe content violates their personal legal rights or applicable local laws.

WhatsApp reviews and responds to valid legal orders from authorities in countries where we operate, where we may receive orders to restrict access to WhatsApp Channels. We assess the legitimacy and completeness of a government request before taking action.

2. IDENTIFYING, REMOVING, ACCESS RESTRICTION OR PREVENTING THE REAPPEARANCE OF TERRORIST CONTENT

Article 7(3)(a) information about the hosting service provider's measures in relation to the identification and removal of or disabling of access to terrorist content;

Article 7(3)(b) information about the hosting service provider's measures to address the reappearance online of material which has previously been removed or to which access has been disabled because it was considered to be terrorist content, in particular where automated tools have been used.

To adhere to locally required laws and sanctions obligations, we use a global definition for terrorist organizations and individuals: "any non-state actor that:

- Engages in, advocates or lends substantial support to purposive and planned acts of violence,
- which causes or attempts to cause death, injury or serious harm to civilians, or any
 other person not taking direct part in the hostilities in a situation of armed conflict,
 and/or significant damage to property linked to death, serious injury or serious harm to
 civilians
- with the intent to coerce, intimidate and/or influence a civilian population, government or international organization
- in order to achieve a political, religious or ideological aim."

© 2024

Under the Whatsapp Channels Guidelines, we take action on:

- Illegal content, content that engages in illegal activity, or that supports violent extremist, criminal organizations or individuals.
- Content that constitutes a credible threat to public or personal safety, incitement of violence, organization or coordination of violent or criminal activities, or that encourages suicide or self-injury.

We have developed our processes and techniques to detect dangerous organizations and terrorist content. Measures to identify and remove or restrict access to terrorist content, individuals, or organizations include:

- Automated and proactive at-scale detection
- Manual human review
- User reports
- Legal orders

We deploy a range of measures to address the reappearance of terrorist content, individuals, or organizations; for example we proactively detect terrorist content and take appropriate measures, which could include removing the content or restricting the user from WhatsApp.

3. REMOVALS, ACCESS RESTRICTION AND APPEALS

Article 7(3)(c) the number of items of terrorist content removed or to which access has been restricted following removal orders or specific measures, and the number of removal orders where the content has not been removed or access to which has not been restricted pursuant to the first subparagraph of Article 3(7) and the first subparagraph of Article 3(8), together with the grounds therefor;

Article 7(3)(d) the number and the outcome of complaints handled by the hosting service provider in accordance with Article 10;

Article 7(3)(g) the number of cases in which the hosting service provider reinstated content or access thereto following a complainant by the content provider.

© 2024

For the period of 1 January 2023 to 31 December 2023, we have no data to include with regard to Articles 7(3)(c), (d), and (g).

4. ADMINISTRATIVE OR JUDICIAL REVIEW PROCEEDINGS

Article 7(3)(e) the number and the outcome of administrative or judicial review proceedings brought by the hosting service provider;

Article 7(3)(f) the number of cases in which the hosting service provider was required to reinstate content or access thereto as a result of administrative or judicial review proceedings.

For the period of 1 January 2023 to 31 December 2023, no administrative or judicial review proceedings were issued. On this basis, we have no further information to include with regard to Articles 7(3)(e) and (f).

© 2024