GNI Statement on Europe's Proposed Regulation on Preventing the Dissemination of Terrorist Content Online

Following the recent agreement by the European Council on a draft position for the proposed regulation on "preventing the dissemination of terrorist content online,"[1] which adopted the initial draft presented by the European Commission with some changes, the Global Network Initiative (GNI) is concerned about the potential unintended effects of the proposal and would therefore like to put forward a number of issues we urge the European Parliament to address as it considers it further.

GNI members recognize and appreciate the European Union (EU) and member states' legitimate roles in providing security, and share the aim of tackling the dissemination of terrorist content online. However, we believe that, as drafted, this proposal could unintentionally undermine that shared objective by putting too much emphasis on technical measures to remove content, while simultaneously making it more difficult to challenge terrorist rhetoric with counter-narratives. In addition, the regulation as drafted may place significant pressure on a range of information and communications technology (ICT) companies to monitor users' activities and remove content in ways that pose risks for users' freedom of expression and privacy. We respectfully ask that EU officials, Parliamentarians, and member states take the time necessary to understand these and other significant risks that have been identified, by consulting openly and in good faith with affected companies, civil society, and other experts.

Background on the Proposal

This regulation follows previous EU efforts to reduce the proliferation of extremist content online, including the EU Internet Forum, launched in December 2015,[2] and the March 2017 directive on combating terrorism.[3] However, the proposed regulation would move beyond the voluntary cooperation[4] underpinning previous initiatives and require member states to

[1] The Council's agreed "General Approach" can be found here: http://data.consilium.europa.eu/doc/document/ST-15336-2018-INIT/en/pdf

[2] http://europa.eu/rapid/press-release_IP-15-6243_en.htm.

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32017L0541&from=EN.

[4] For an analysis of the possible movement from notions of responsibility to legal liability in the proposed legislation, see, *e.g*, this study from Stanford CIS Intermediary Liability Fellow Joan Barata: http://cyberlaw.stanford.edu/publications/new-eu-proposal-prevention-terrorist-content-online-important-mutation-e-commerce and pp. 2-3 of this study by Dr. Alexandra Kuczerawy, https://cdt.org/files/2018/12/Regulation-on-preventing-the-dissemination-of-terrorist-content-online-v3.pdf

establish legal penalties against ICT companies for failure to comply with the obligations outlined in this proposal. GNI joins others who have flagged that more work is needed to analyze the effectiveness of these past approaches before the current proposal can be justified as necessary and appropriate.[5]

This effort also come against a backdrop of separate initiatives by the European Commission to address other areas of "controversial content" online, including the May 2016 "Code of Conduct for Addressing Hate Speech Online", the March 2018 "Recommendation on measures to effectively tackle illegal content online," and the September 2018 "Code of Practice to address the spread of online disinformation and fake news."

GNI's Work on Extremist Content to Date

GNI is the world's preeminent multistakeholder collaboration in support of freedom of expression and privacy online. GNI's members include leading academics, civil society organizations, ICT companies, and investors from across the world. All GNI members subscribe to and support the GNI Principles on Freedom of Expression and Privacy ("the Principles"), which are drawn from widely-adopted international human rights instruments. The Principles, together with our corresponding Implementation Guidelines, create a set of expectations and recommendations for how companies should respond to government requests that could affect the freedom of expression and privacy rights of their users. The efforts of our member companies to implement these standards are assessed by our multistakeholder board every other year.

In July 2015, GNI launched a policy dialogue — which began internally, and later expanded to include external stakeholders, including the European Commission and some member states — to explore key questions and considerations about government efforts to restrict online content with the aim of protecting public safety, and to discuss the human rights implications of such government actions. In December 2016, GNI released a policy brief, "Extremist Content and the ICT Sector," that was informed by that dialogue and included recommendations for governments and companies to protect and respect freedom of expression and privacy rights when responding to alleged extremist or terrorist content online.[6] We refer to these

[5] *See, e.g.*, https://www.accessnow.org/joint-letter-opposing-the-proposed-terrorist-content-regulation/.
[6] https://globalnetworkinitiative.org/gin_tnetnoc/uploads/2016/12/Extremist-Content-and-ICT-Sector.pdf.

recommendations as a basis to highlight the following elements in the proposed regulation which remain a potential concern.

Definitional Challenges

In our policy brief, GNI noted that laws that prohibit incitement to terrorism "should only target unlawful speech that is intended to incite the commission of a terrorist offense and that causes a danger that a terrorist offense or violent act may be committed." While the Council's amendments clearly try to add greater definitional clarification to the requirement for "intent," the regulation continues to reference the definition of "terrorist content" found in Directive (EU) 2017/541, which has been deemed problematic by human rights groups and independent experts.[7] In addition, because this definition is based in a Directive, it creates the possibility that it will be interpreted with significant variance across member states.[8] These definitional issues are likely to lead to legal uncertainty, as well as potentially overly-aggressive interpretations by companies that could result in the removal of content that should be protected under the Charter of Fundamental Rights and Member State constitutions. Notably, and unlike the definition of terrorist offenses in the Directive, the definition of terrorist content in the regulation does not clarify that content must amount to a criminal offense or be punishable under national law.[9]

GNI notes in our extremist content brief that laws and policies should clearly distinguish between "messages that aim to incite terrorist acts and those that discuss, debate, or report them." Because the regulation fails to make such a clear distinction, it will pose particular risks to the legitimate expression of journalists and researchers working on documenting terrorist abuses. It may also, unintentionally, impact those working on counter-terrorism efforts, including those trying to use arguments based in humor, satire, or religious doctrines to engage in counter-messaging or counter-narrative efforts.

---

[7] *See, e.g.*, Human Rights Watch, et al, "EU Counterterrorism Directive Seriously Flawed," available at: https://www.hrw.org/news/2016/11/30/eu-counterterrorism-directive-seriously-flawed#; and Kaye, Cannataci, and Aoláin Letter, pp. 2-4, available at: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24234

[8] *See* "GSMA/ETNO position paper on the European Commission's Proposal for a Regulation on preventing the dissemination of terrorist content online," pp. 2-3, available at: https://etno.eu/datas/positions-papers/2018/ETNO%20GSMA%20Position%20Paper%20on%20Preventing%20terrorist%20content%20online.pdf.

[9] *See* pp. 6-8 of Dr. Aleksandra Kuczerawy https://cdt.org/files/2018/12/Regulation-on-preventing-the-dissemination-of-terrorist-content-online-v3.pdf

Removal Orders

The proposal allows designated "competent authorities" to issue removal orders to companies requiring they remove terrorist content, deemed illegal under the proposed regulation, within one hour from receipt of the order. As noted in our policy brief, GNI members are expected to "interpret government restrictions and demands, as well as governmental authority's jurisdiction, so as to minimize the negative effects on freedom of expression." The rapid timeline prescribed potentially creates significant challenges for appropriate review of removal orders.

In addition, the potentially significant legal penalties for noncompliance will put increased pressure on companies to comply with these orders. While we appreciate the provisions, particularly in the Council's amendments, allowing for companies to appeal such orders to the judicial authority of the member state that issued the request, it is not clear that this appeal delays the timeline for removal.[10] If content is removed, the amount of time it can take for appropriate redress to take place and for content to be reinstated poses substantial freedom of expression risks.[11]

Finally, GNI members have also worked extensively to understand and address the jurisdictional challenges that emerge when governments make orders that end up being enforced through or having impacts on other jurisdictions.[12] While the provision for a "consultation procedure" added by the Council is helpful, the proposal still creates significant potential for conflicts of laws to emerge, which would add to the aforementioned lack of legal clarity.

Referrals

The proposed regulation would allow member states to establish "competent authorities" to issue referrals of content "that may be considered terrorist" for review by companies under their own terms and conditions, and if appropriate, removal. As others have noted, it is not clear if competent authorities or member states are expected to have already determined that

[10] *See* pp. 9-10 of this analysis by Dr. Aleksandra Kuczerawy https://cdt.org/files/2018/12/Regulation-on-preventing-the-dissemination-of-terrorist-content-online-v3.pdf
[11] *Ibidem* pp. 9-10
[12] *See, e.g.*, "Global Network Initiative Submission to the European Commission Consultation on the Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters," available at: https://ec.europa.eu/info/law/better-regulation/feedback/12963/attachment/090166e5bc5c2bc5_en.

the content is illegal under national law prior to submission of a referral.[13] The law also requires companies to establish "operational and technical measures facilitating expeditious assessment of content sent by competent authorities."

In "Extremist Content and the ICT Sector," we raised concerns about the potential for this type of referral to "set precedents for extra-judicial government censorship without adequate access to remedy, accountability, or transparency for users and the public." GNI has called on governments to use formally established legal procedures when they demand the restriction of content by ICT companies, to adopt additional safeguards, and to be clear about whether they are issuing referrals or issuing legal orders, and it would appear that these referrals do not meet that standard. It is also unclear if there would or could be any independent, judicial oversight of this mechanism, and yet the proposal notes that lack of expeditious response could lead to the implementation of proactive measures or even legal penalties.[14]

Duties of Care/Proactive Measures

GNI noted in "Extremist Content and the ICT Sector" that governments should not pressure companies to change their terms of service. Yet, Article Three of the proposal establishes "duties of care" whereby companies are expected to undertake reasonable and proportionate actions in accordance with the regulation for the removal of extremist content on their platforms, and furthermore, are expected to "include, and apply, in their terms and conditions provisions to prevent the dissemination of terrorist content."

Beyond these "duties of care," the proposed regulation also outlines an expectation for companies to undertake "effective and proportionate" "proactive measures to protect their services against the dissemination of content," including through automated means. While the Council's position notes that this requirement is "depending on the risk and level of exposure to terrorist content," this fails to clarify if, when, and how companies should take such measures. Should a company receive a removal order under Article Four, they are required to implement these proactive measures, both to prevent re-upload of the content that was identified in a previous removal order, and on terrorist content more broadly, reporting back to the

[13] *See, e.g*, Kaye, Cannataci, and Aoláin Letter, p. 7, available at: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24234
[14] *See* p. 8 of UN Special Rapporteurs Kaye, Cannataci, and Aoláin report on the proposal: https://spcommreports.ohchr.org/TMResultsBase/DownLoadPublicCommunicationFile?gId=24234

competent authority within three months about the proactive measures in place for "detecting, identifying, and expeditiously removing or disabling access to terrorist content."

This aspect of the proposal poses an increased risk on the right to privacy, in so far as it calls on companies to proactively monitor and filter their users' communications. Furthermore, as the proposal acknowledges, it "could derogate" from the provisions against a "general monitoring obligation" in Article 15 of the e-Commerce Directive, "as regards certain specific, targeted measures, the adoption of which is necessary for overriding public security reasons" (see recital 19). Finally, it is important to recognize the potential freedom of expression risks that come from a reliance on automated filtering measures. The existing limitations on the effectiveness of existing technology to search, analyze, and filter content online are often underappreciated and can lead to over-removal of legitimate content.[15]

Transparency & Redress

GNI would like to emphasize the critical need to ensure adequate redress and transparency measures are in place throughout the various elements of this proposal. The proposal clarifies requirements for companies to make available the reason for content removals, as well as avenues for content providers to contest the decision. However, there are no similar requirements for the competent authorities, and as previously noted, any appeals to member states' judicial authorities under Article Four do not necessarily delay the timeline for decision. In sum, the proposal's repeated reference to users' right to remedy and the provisions on redress do not seem to be matched by specific guidance and effective implementation.[16]

In our policy brief, GNI members flagged that "governments should regularly and publicly report, at a minimum, the aggregate numbers of requests and/or legal orders made to companies to restrict content and the number of users impacted by these requests," and with regards to the requests for removal made under companies' terms of service, "Governments should regularly and publicly report, at a minimum, the aggregate number of requests made to companies to restrict content and the number of users impacted by these requests." While we appreciate that the transparency obligations for companies under Article Eight include a

[15] *See, e.g.*, Center for Democracy and Technology, "Mixed Messages: the Limits of Automated Social Media Content Analysis," available at: https://cdt.org/insight/mixed-messages-the-limits-of-automated-social-media-content-analysis/.
[16] *See* pp. 9-10 of this report by Dr. Aleksandra Kuczerawy: https://cdt.org/files/2018/12/Regulation-on-preventing-the-dissemination-of-terrorist-content-online-v3.pdf

requirement to report on the "number of pieces of terrorist content removed or to which access has been disabled, following removal orders, referrals, or proactive measures, respectively," there is little in the way of similar requirements for governments anywhere in the proposal. Under the current proposal, the obligatory government reporting only appears to apply for the purposes of assessing the proposal's implementation and effectiveness, not for providing transparency for users and the general public.

Practical Issues

GNI would also like to flag some potential ambiguities in implementation that pose risks for users' rights. First, there is very limited guidance for member states' designation of competent authorities who carry out the provisions under Articles Four, Five, and Six. While Article 17 states that all member states must designate a competent authority or competent authorities and notify the Commission, the only requirements seem to be that competent authorities are "administrative, law enforcement or judicial authorities" (see recital 13). Furthermore, states are able to designate multiple competent authorities, which could cause confusion for companies receiving requests. Several companies' have stated that the member states should be required to establish a single authority, which would seem a reasonable request.[17]

Second, there are stringent requirements for companies to establish legal representatives to "ensure compliance with enforcement of the obligations under this regulation" (See recital 35), as well as points of contact to "facilitate the swift handling of removal orders and referrals," including the one-hour timeline. In addition, the definition of "hosting service providers" in the regulation has been criticized for its lack of clarity as to what companies are covered under the proposal.[18] In combination, these two issues pose potential challenges for smaller and medium sized enterprises, who may not have the existing infrastructure to deal with the rapid, 24/7, requests and properly assess the potential human rights impacts, or may be discouraged from potential business opportunities at the cost of compliance with this regulation.

[17] *See, e.g.*, p. 3 of the GSMA/ETNO joint position paper: https://etno.eu/datas/positions-papers/2018/ETNO%20GSMA%20Position%20Paper%20on%20Preventing%20terrorist%20content%20online.pdf
[18] *Ibidem* p. 2

Conclusion

As noted above, the proposed regulation raises significant issues that must be addressed before it is enacted into law. At a minimum, amendments should: (i) ensure key provisions, such as the definitions of terrorist content, hosting service providers, and competent authorities are refined and clarified; (ii) clarify that legal challenges of content removal orders by companies will toll the 24-hour clock for related removals; (iii) require that content referrals under the regulation are reviewed against relevant laws and appropriate oversight mechanisms are in place for referrals; (iv) remove requirements that companies modify their terms and conditions; (v) eliminate, or significantly limit, situations where companies will be ordered or expected to implement "proactive measures" against their will; and (vi) strengthen provisions on remedy and transparency, including vis-a-vis government decisions.

GNI recognizes the importance of taking measures to prevent the dissemination of terrorist content online and stands ready to continue engaging with relevant actors, including the Council, the Commission, and Parliament to ensure that our collective efforts to address this challenge remain effective, efficient, and consistent with applicable human rights principles.