Global Network Initiative Submission to the European Commission Consultation

Proposal for a Regulation on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive on laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings

1. Introduction

The Global Network Initiative (GNI) welcomes the opportunity to participate in the public consultation on the European Commission's proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters and the proposal for a Directive on laying down harmonized rules on the appointment of legal representatives for the purpose of gathering evidence in criminal proceedings. GNI is a multistakeholder initiative composed of companies in the information and communications technology (ICT) sector, human rights and press freedom civil society organizations, academics, and socially responsible investors. GNI members work collaboratively through internal and external engagement to promote and protect freedom of expression and privacy in the ICT sector.

GNI was pleased to have submitted previous comments to this process in October 2017; that feedback is incorporated here by reference.[1] As we noted in that submission, GNI members consider the following, non-exhaustive list of measures and commitments critical to the design and implementation of legal procedures for facilitating cross-border requests for electronic evidence by law enforcement authorities for criminal matters consistent with international human rights law: independent prior authorization of requests; focus on serious crimes; availability of meaningful redress; transparency regarding the number, type, and scope of the requests; and oversight and accountability to regularly ensure that requests meet such requirements.

2. Positive Takeaways

GNI commends the Commission's open consultation with stakeholders throughout this process. GNI specifically appreciates the use of both open and targeted surveys, bilateral and expert meetings, conferences, and an independent assessment, which set a good precedent for future regulatory developments.

[1] GNI Submission to the European Commission Consultation: Improving Cross-Border Access to Electronic Evidence in Criminal Matters, available at: https://globalnetworkinitiative.org/gin_tnetnoc/uploads/2018/03/GNI-submission-EC-cross-border-e-evidence-consultation-oct2017.pdf

References to the protection of fundamental rights, transparency, and accountability in the text of the Directive and Regulation are welcome, appropriate, and aligned with the GNI Principles.[2] Similarly, the acknowledgement of potential conflicts of obligations with third country law and the corresponding inclusion of a judicial review process is commendable. GNI also appreciates that the proposed European Production Orders for transactional and content data would be restricted to certain serious crimes and require the prior approval of a judicial authority.

Finally, the Proposal's focus on cross-border data requests to acquire stored data and the decision not to expand the framework to include matters such as direct access to remotely stored data is commendable.[3] GNI urges the Commission to maintain this focused approach, which is the best way to ensure flexibility and respect internationally recognized human rights principles in regulatory approaches that impact rapidly changing and nuanced technologies.

3. Recommendations

In reviewing the Proposal, GNI identified several areas of ambiguity that would benefit from improvement during the legislative process. These represent opportunities to further clarify and strengthen the value and ease implementation of the new process.

The GNI Principles 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, consistent with the UN Guiding Principles on Business and Human Rights. As the GNI Principles evidence, ICT companies can and often do play an important role in ensuring that government requests for user data are consistent with domestic law and international human rights principles. Efforts, including these proposals, to facilitate such requests across borders may help expedite legitimate law enforcement investigations, but they also introduce increased risks to user rights. As a result, the Commission must ensure (i) that the responsibility falls squarely on issuing authorities to ensure that EPOs are consistent with domestic law and the Charter of Fundamental Rights, and do not constitute manifest abuse; (ii) that compliance with EPOs does not create liability for providers; and (iii) that providers have

[2] GNI Principles on Freedom of Expression and Privacy, available at: https://globalnetworkinitiative.org/sites/default/files/GNI-Principles-on-Freedom-of-Expression-and-Privacy_0.pdf

[3] Notwithstanding the fact that the Commission has commendably decided not to address "direct access", the GNI would like to direct the European Commission to certain confusion generated by the use of the term "direct access," since that language continues to be used in the context of cross-border e-evidence discussions. The definition in the European Union's impact assessment for this Regulation—"cases where authorities access data without the help of an intermediary, for instance following the seizure of a device ("extended search") or following the lawful acquisition of login information ("remote search")"—appears to be focused on accessing data on a device or in the "cloud," but could also be read to include efforts to access data in transit across networks. This latter category is what others have used the term "direct access" to refer to. See, e.g., https://www.telecomindustrydialogue.org/wp-content/uploads/Industry-Dialogue-reply-to-Privacy-International-Feb-8-2017.pdf. Future discussions should make very clear what is and is not being contemplated when this term is utilized.

sufficient information and opportunity to assess and respond to EPOs consistent with relevant laws, their responsibility to respect human rights,[4] and legitimate user expectations.

Specifically, the GNI recommends that (1) **appropriate safeguards should be built in** to the final regulation to ensure that orders served on providers will be clear and narrowly tailored to the crime being investigated so as not to create legal uncertainty and undue burden on service providers, or elicit responses from service providers that unduly interfere with the privacy interests of their users. The Commission should also consider amending the regulation to (2) require, consistent with EU law,[5] that the **subject of the data request be given notice** in a manner that does not compromise the investigation. In addition, the Commission should (3) ensure that the **enforcing state is provided adequate notice** of relevant orders.

The GNI is also concerned that the high bar required under the Regulation to challenge orders on human rights grounds ("if, based on the sole *information* contained in the European Production Order Certificate (EPOC), it is apparent that it *manifestly violates* the Charter or that it is *manifestly abusive*…") might deter providers of all sizes and types from challenging orders and would thereby undermine protections for users' human rights. The Commission should therefore (4) **ensure that the grounds for challenging EPO are clear and that companies have sufficient information** to enable them to understand whether a given order is authentic and lawful.

In addition, (5) **the time frames should be relaxed** in the final regulation to permit providers to assess the orders they receive and prioritize the most critical requests. Furthermore, the final regulation (6) should **ensure a substantial level of harmonization** is specified in order to minimize the risk of forum shopping. It is also of the utmost importance to (7) ensure that transmission of EPOs and responses are secure, including by facilitating access to secure transmission methods for smaller companies. The Commission should also (8) consider limiting the number of authorities that member states may identify as competent to issue and/or validate EPOs. Finally, the proposed Regulation only mentions that possible reimbursement schemes should be determined through national Law. Instead, (9) the Regulation should **foresee a mandatory harmonized reimbursement calculation**.

4. Additional Concerns

[4] As set out in the UN Guiding Principles on Business and Human Rights [United Nations Office of the High Commissioner for Human Rights, *Guiding Principles on Business and Human Rights: Implementing the United Nations "Protect, Respect and Remedy" Framework*, HR/PUB/11/04 (New York and Geneva: United Nations, 2011) https://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf], and the Global Network Initiative Principles [https://globalnetworkinitiative.org/gni-principles/] and Implementation Guidelines [https://globalnetworkinitiative.org/implementation-guidelines/].

[5] See the ECTR ruling in *Szabó and Vissy v. Hungary*, (para. 86) and the CJEU ruling in the combined judgment in *Tele2 Sverige AB v. Post- och telestyrelsen* and *Secretary of State for the Home Department v. Tom Watson et al.*, (para 121).

The Directive's reliance on minimal connecting factors when requiring the appointment of legal representatives for providers that offer services in EU Member States may place undue burden on small smart-ups, both in terms of the requirement to have a legal representative in-country and the costs incurred when reviewing and executing orders. Such a burden could leave smaller providers ill-equipped to diligently respond to an influx of insufficiently supported production or preservation orders, which, in turn, may pose threats to their users' human rights.

Specific design elements of the draft forms included in the proposed Regulation may also inadvertently lead to inappropriately broad requests for information. Section D of the EPOC form, provided in the Annex to the proposed Regulation, lists many possible types of electronic evidence to be requested, which may in practice encourage judges or prosecutors to over request information out of convenience rather than conducting a careful analysis of what information is strictly necessary and proportionate in a given instance.

GNI also has concerns about the low level of protection contemplated for EPOCs for Access Data, which appears to be based on the Proposal's unsubstantiated and categorical assertion that "subscriber and access data are less sensitive." In GNI's experience, this may not always be the case. In particular cases, subscriber and access data—especially when gathered in large volumes and/or over long periods of time—can significantly implicate privacy considerations. Recent high-court decisions in various jurisdictions reflect a recognition of and move toward greater protections for sensitive, non-content digital information.[6] Accordingly, GNI recommends greater protection of user Access Data.

Finally, the proposed Regulation's annual reporting is insufficiently transparent. The Regulation requires Member States to report annually to the European Commission but does not require public disclosure of that information. Transparency requires open communication with the public, not just government bodies.

5. Conclusion

We look forward to continuing to engage constructively with the Commission, EU Member States, foreign governments, multilateral organizations, and other critical stakeholders on this issue. GNI appreciates the European Commission's consideration of these comments.

---

[6] See, e.g. *Eur. Court of HR, Benedik v. Slovenia, judgment of 24 April 2018, application no. 588/13*, a 2018 European Court of Human Rights decision which found the failure of the Slovenian police to obtain a court order to access subscriber information associated with a dynamic IP address to be a violation of Article 8 of the EU Charter (right to respect for private and family life; *C-293/12 AND C-594-12, DIGITAL RIGHTS IRELAND LTD V. IRELAND, 8.4.2014 ("DRI")*, a 2014 European Court of Justice decision which found an EU directive requiring ISPs to store telecommunications data to facilitate the prevention and prosecution of crime to be invalid under Articles 7 and 8 EU Charter; and *Carpenter v. United States, No. 16-402, 585 U.S. ____ (2018)*, a 2018 U.S. Supreme Court ruling which held that the accessing of historical records containing the physical locations of cell phones without a search warrant violates the Fourth Amendment of the United States Constitution.