ETNO position paper on improving cross-border access to electronic evidence in criminal matters

Law Enforcement and Judicial Authorities increasingly rely on the analysis of data generated by the widespread use of electronic communications services and devices. The ability of individuals and organisations to easily store and share data across borders, through major service providers that often operate from outside the European Union, means that even an ordinary crime with a clear national or local dimension can easily acquire a transnational relevance.

While ETNO acknowledges the importance for Law Enforcement and Judicial Authorities to have the right tools to investigate and prosecute serious crime, legal certainty is crucial especially when such tools may affect individuals' fundamental rights. Therefore, ETNO calls for more legal certainty and clear and feasible provisions in the proposed Regulation on cross-border access to e-Evidence that reduce the burden on service providers.

ETNO fears that the proposal, as initially presented by the Commission, may decrease legal certainty for service providers compared to today's situation. ETNO calls on EU co-legislators to consider carefully some necessary changes in order to improve the e-Evidence Regulation:

- **More accountability for Member States:** it should be up to the Judicial Authorities, and not to service providers, to ensure that requests for e-evidence are compliant with the Charter of Fundamental Rights of the EU and with the local law of the issuing authority.
- **Increase legal certainty:** include a detailed list of criminal offences in the scope of the Regulation; require judicial oversight for all types of data. Include harmonised provisions with respect to requests for information related to specific targeted professions/groups (lawyers, journalists, etc.), where such provisions are provided for in national law.
- **Improve the feasibility of provisions, addressing concrete issues** related to: conflicting laws in the EU and compatibility with international law, costs (re-imbursement of both OPEX and CAPEX), short delays, delivery authenticity, and process to challenge orders that are not conforming. Establish a specialised Court and a secure transmission channel for the handling of requests.

EUROPEAN TELECOMMUNICATIONS Network Operators' Association A.I.S.B.L
Boulevard du Régent 43-44, 1000 Brussels, Belgium I Tel: +32 (0)2 219 3242 I www.etno.eu

GENERAL COMMENTS

The e-Evidence package aims to provide legal certainty and efficiency to the tools used in Europe to investigate serious crime in the digital age. ETNO has always fully supported such an imperative objective. By virtue of their compliance with EU and national legal obligations, European telecommunications operators have a long experience in supporting Law Enforcement and Judicial Authorities in criminal investigations.

Despite the rise in the number and complexity of requests, ETNO members have always responded efficiently and promptly to both domestic and international requests for e-evidence. Telecom operators are willing to continue cooperating with Law Enforcement and Judicial Authorities. For that, we need a legal framework that provides legal certainty and sets out clear, unambiguous, understandable, and legally sound orders and cost reimbursement schemes.

ETNO would like to highlight that the delays that the proposed e-Evidence Regulation aims to reduce are not due to telecom operators, but to the functioning of the Judicial Administration and its lengthy processes.

Existing cooperation mechanisms for the cross-border exchange of information in the context of criminal investigations within the EU **should be improved and streamlined** before proposing new instruments. In Directive 2314/41/EU regarding the European Investigation Order in criminal matters (**EIO Directive**), the distribution of tasks and the coordination between the issuing and the executing Judicial Authorities are crucial as they ensure fundamental rights' safeguards for individuals and legal certainty for service providers. However, the proposed e-Evidence Regulation circumvents such tasks, eliminating the role of the executing Authority and delegating individuals' safeguards to private companies.

ETNO believes that the role of both the issuing and the executing Judicial Authorities are indispensable as "double protection" and that the current EIO process should be streamlined rather than circumvented. Another reason for improving the current process is that the EIO Directive has a broader scope than the e-Evidence Regulation. Since only the EIO Directive addresses wiretapping, it will remain very much in use.

Member States had to transpose the EIO Directive into national laws by May 2017 and some Member States have not transposed it yet. The EIO Directive needs more time before a complete assessment evaluating its application in practice, its weaknesses and strengths can be made. However, the tasks and the coordination between issuing and the executing Judicial Authorities could already be accelerated; otherwise, Authorities will prefer to avail of the speedy EPO instead of going through a lengthier EIO procedure.

As a second step, once the processes provided by the EIO Directive reviewed and streamlined, the proposed e-Evidence Regulation should build upon the more expedite, but still managed by Judicial Authorities, mechanisms of the EIO Directive. This would avoid delegating to industry the management of individuals' fundamental right safeguards. ETNO opposes any form of privatised law enforcement that might undermine the fundamental rights of those that are subject to investigative measures.

Nonetheless, if the European co-legislators decide that adopting the e-Evidence Regulation provide an added value, ETNO proposes that at least the following concrete proposals are taken into account to improve the proposal.

SPECIFIC COMMENTS

- **More accountability for Member States**

  - **Art. 14 on enforcement.** ETNO calls for the redrafting of this provision as it should be up to Judicial Authorities, and not to service providers, to assess a European Production Order (EPO)'s compliance with the Charter of Fundamental Rights of the EU and with the local law of the issuing authority.

    The role that the proposal foresees for service providers seems unrealistic. Telecom operators are not in a position to guarantee, for example, that the order does not violate the Charter. Similarly, the authenticity and legal validity of the orders (check of the issuing Authority or check that the criminal offence is punishable with a 3-year custodial sentence in the issuing Member State) should not be a responsibility of the operators. Moreover, in practice, this role would impose an excessive administrative burden and important costs for the service providers. Therefore, **industry thus cannot replace Judicial Authorities** in their key role of assessing compliance of an EPO.

  - **Secure authentication and transmission mechanisms.** It would be crucial to build a centralized secure transmission channel, a sort of **unique platform**:

    - receiving the requests from Law Enforcement Authorities of the issuing Member State;
    - checking the validity of the request, in accordance with Art. 9, via a competent Judicial Authority in the enforcing Member State; and
    - forwarding the requests to the service provider.

    In essence, a service provider should always answer to an Authority that has the judicial power to check the validity of the requests. The platform will then ensure that the request is authentic, adequate and can be met, avoiding that this burden is put on service providers. In addition, this

would allow service providers to have a unique, secure entry point. Currently, the Commission is working on an e-CODEX Regulation that will complement the EIO Directive, with a view to improve the current exchange of information among Member States. This secure exchange platform could be opened up to private companies for the secure exchange of information between competent Authorities and service providers. This would provide legal certainty to service providers and Law Enforcement Authorities. For that, it should be necessary that the e-CODEX Regulation and its implementation be ready by the time the e-Evidence Regulation becomes applicable.

- In a transitional phase before the secure platform is established and operational, it could be important to constitute a **Judicial Single Point of Contact** in each Member State, charged to receive and validate the transmission of other Member States' requests to the national service providers. National service providers would then only be subject to the request of this entity in addition to the national requests in purely domestic cases. This would also allow an early involvement of the Authority of the enforcing Member State, which would assess if the Order were in conflict with the Charter or with national law or interests. However, in the current proposal, the Authority of the enforcing Member State only intervenes when there is a problem and the process is already delayed. Therefore, the establishment of a Judicial Single Point of Contact would not imply lengthier processes, but on the contrary, it would add more efficiency to the process.

- **"Good faith clause"**. In light of the above, although we welcome the "good faith clause" of Recital 46, we believe that legislators should render the limitation of responsibility for service providers that comply with an EPO in good faith more explicit and robust. This clause should also clarify that providers are not required to assess the grounds for the necessity and proportionality of the EPO.

- **<u>Increase Legal Certainty</u>**

  - **Art. 5 on EPO conditions.** ETNO supports the inclusion of **a detailed list of criminal offences** covered by the e-Evidence Regulation instead of relying on the length of the minimum sentence to establish the gravity of a crime. Moreover, Art. 5 already provides an initial list of some offences identified in EU Law and covered by the Regulation. This list should be completed and could build upon the list of criminal offences mentioned in Annex D of the EIO Directive (e.g.: participation in a criminal organisation, terrorism, trafficking in human beings, sexual exploitation of children and child pornography, illicit trafficking in narcotic drugs and psychotropic substances, computer-related crime, etc.). This "catalogue" of crimes covered by the Regulation would help ensure a common interpretation and would enhance legal certainty for service providers and Authorities. We see no justification for having a different list of criminal offences in the EIO Directive and in the e-Evidence Regulation, as both laws serve the same objective.

In addition, the forthcoming European Court of Justice (ECJ) Ruling on Case C-2017/16 relating to the definition of serious crime that can justify access to telecom data might have a broad impact on the ongoing discussions on the e-Privacy Regulation, Data Retention and e-Evidence[1].

- **A judicial authorisation should always be necessary.** This is important also regarding the distinction proposed by the Commission between subscriber/access data and transactional/content data and especially because for subscriber and access data, no Court order is needed. It is important to stress the difficulties to clearly distinguish in practice between "access" and "transactional" data (e.g.: date, time of the communication is "access" or "transactional" data?). The old Data Retention Directive (2006/24/EC), without explicitly defining these two categories of data, did already refer to both "access" and "transactional" data. This is important here because both categories imply different treatment (Prosecutors can issue an EPO for access data without judicial oversight).

  The text should simplify the categorization of data. More importantly, it is necessary to have **judicial oversight for all requests, related to a determined list of offences and for all data categories** in order to ensure a harmonized interpretation that would enhance certainty.

- **<u>Improve the feasibility of provisions by addressing concrete issues</u>**

  - **Costs.** Compliance with the new provisions will require substantial capital and operational costs by telecom operators. ETNO members are concerned with being confronted with requests from multiple Authorities of different Member States, with concrete possibility of forum shopping cases (it could be easier in some jurisdictions to get access to e-evidence due to the differences in material law across the EU). In this respect, it is important to clearly limit when Production and Preservation Orders can be issued. The new rules will change the current situation in which telecoms are only obliged to respond to requests of their local Authorities.

    At the same time, this increase of requests and, more importantly, the need to transmit the requested information in a secure manner and invest in secure transmission channels will imply additional costs for the industry. The Regulation should foresee a comprehensive and **harmonised reimbursement mechanism** to ensure that the costs incurred by telecom operators to make these proposals effective are fully covered. Cost reimbursement is not only crucial from an industry perspective, but it ensures that requests to e-evidence are kept limited to what is strictly necessary

[1] On 3 May, the Advocate General published his Conclusions on Case C-2017/16 considering that even criminal offences that are not particularly serious may justify disclosure of basic electronic communications metadata provided such disclosure does not seriously undermine the right to privacy, guaranteed by the e-Privacy Directive and by the Charter.

in a criminal investigation and ensure more accountability for e-evidence requests. This is relevant from the point of view of full respect of fundamental rights. This is also important considering that, even if the scope of the current proposal is limited to Member States, at the same time the scope may be enlarged to all signatories of the Budapest convention and extended via bilateral agreements (e.g.: US CLOUD Act).

- **Single format**. It is not practical for telecom operators to support the multiple national language and disclosure handover formats in use throughout the EU. Therefore, either the Regulation defines a single pan-European request and response format, with no national options or variance, or telecom providers should be free to use one or more national formats of their choice. Format conversation must be the responsibility of the requesting Law Enforcement Authority and not the telecoms operators.

- **Timeframes**. The proposed Regulation establishes very short timeframes for response (10 days upon receipt of an EPO or within 6 hours in emergency cases), which will make it difficult to assess and verify whether the EPO fulfils all the necessary legal requirements. The Regulation should recognise the limited resources of service providers to process these requests, especially regarding emergency cases. Such short timeframes might imply that service providers have to prioritise the requests coming from Authorities from another Member State over requests from national Authorities, which might also face emergency cases. Regarding European Preservation Orders, it should be avoided that the Regulation be misused to allow data retention, if the Order is not confirmed by a EPO but is rather extended just before the foreseen 60 days.

- **International dimension**. The future e-Evidence Regulation cannot be considered in isolation, but it relates to existing and proposed rules at the EU and international levels (GDPR, proposed e-Privacy Regulation, US CLOUD Act and even national laws on data retention where they exist). It is crucial to avoid conflicts of law (e.g.: Art. 48 GDPR). Nothing in the US CLOUD Act prohibits EU and US from lawfully negotiating a general framework, with the EU being considered as a "foreign government". Compared with negotiating with each Member States, there could be significant advantages for the US in negotiating with the EU as a whole. Any agreement on law enforcement transfers of data will only succeed if it passes muster under EU Law.

- **Encryption**. European Production or Preservation Orders should always be addressed to the service providers that may be able to decrypt encrypted e-Evidence. Further to Recital 19 that states that data should be provided regardless of whether it is encrypted or not, the future Regulation should make absolutely clear that ISPs will not be required to decrypt those data.

- **Date of application**. The Regulation should apply from 3 years after its entry into force (instead of 6 months as initially proposed), taking into account the time needed for service providers to

implement all technological tools necessary to deal with both the expected high volume of requirements and the speed of response. This 3-year period would allow the completion and implementation of the e-CODEX Regulation. As a precedent, the EIO Directive established a transposition period of 3 years giving sufficient time for Member States to adopt their respective national laws.

CONCLUSION

ETNO calls for solutions that increase the level of legal certainty for service providers instead of shifting the responsibility to solve the current inefficiencies of cross border investigations from Member States to service providers.

Telecom operators are contrary to any form of privatised law enforcement that might undermine the fundamental rights of those that will be subject to investigation measures, exposing service providers to major new difficulties, as well as civil and criminal liability, not only vis-à-vis Judicial and Law Enforcement Authorities, but also towards public opinion for the possible misuse of their personal data.

ETNO stresses the necessity to implement substantial safeguards to avoid potential risks to the protection of fundamental rights ensuring that confidentiality of communication and right to privacy are not undermined, and trust in telecommunication industry is not broken.