October 2017

ETNO response to the European Commission public consultation on improving cross-border access to electronic evidence in criminal matters

ETNO welcomes this opportunity to comment on the public consultation "on improving cross-border access to electronic evidence in criminal matters" launched by the European Commission as part of the European Agenda on Security. Our Association indeed fully recognises the urgent need to cope with the increasing use of information society services (ISS), especially social media and over-the-top (OTT) messaging services, by criminals to communicate.

Although the consultation is primarily targeted at law enforcement authorities (LEAs) and individual service providers, ETNO would like to provide the Commission with its views to this crucial debate. European telecommunications operators have indeed a long-lasting experience in collaborating with LEAs in criminal investigations, by virtue of their legal obligations and based precisely on a strict compliance with EU and national rules.

Drawing on this experience, ETNO would like to stress two key messages:

- Law enforcement access to data held by providers of electronic communication network and services is already governed by a robust EU and national regulatory framework, which is more stringent than the one applicable to ISS and other digital service providers, which are currently excluded from the most part of this legal framework. We understand that this is precisely the issue that Commission is aiming to tackle. There is thus no need for additional legislation covering the telecoms sector. Any such addition would in fact expose telecom providers to legal uncertainty and potential litigation. Before introducing new rules for ISS and other providers, the expansion of the scope of current ECS-specific laws and policies to these players should be considered.

- Collaboration among LEAs through mutual assistance and international cooperation agreements is paramount to ensure the respect of the fundamental rights of all parties involved and should thus be the rule. The improvement of these legal mechanisms should be prioritised. Any new measure to facilitate cross-border access to electronic evidence (both within the EU and to third countries) should take full account of existing and upcoming EU regulation in the fields of electronic communications, data privacy, and judicial cooperation in criminal matters in order to ensure legal certainty. Fragmented laws and inconsistent protections of data belonging to individuals and organizations in different jurisdictions causes uncertainty and lack of trust in the digital economy.

This input does not address the important issues around data retention and encryption, since they are being addressed by the Commission and Member States in two different work streams. ETNO is following those discussions with great interest and will address them separately at a later stage.

A Robust Framework for ECS

Directive 2002/20/EC on the authorisation of electronic communications networks and services (Authorisation Directive) includes a list of conditions that may be attached to a general authorisation for providing telecommunications services. One of these conditions is the permission of legal interception by competent national authorities in conformity with Directive 2002/58/EC on privacy and electronic communications (e-Privacy Directive) and Directive 95/46/EC on the protection of individuals with regard to the processing of personal data (Data Protection Directive).

The Authorisation Directive is currently being review as part of the reform of the EU regulatory framework for the telecoms sector into a proposed European Electronic Communication Code (EECC). This draft EECC has taken a technology-neutral approach to sector-specific regulation, introducing the definitions of "number-based" and "number-independent" interpersonal communication services (ICS) that also cover services which are considered as functionally equivalent to traditional ECS, such as VoIP and instant messaging.

It is important that all ICS be subject to the general authorisation regime of Article 12 EECC, hence be required to allow for legal interception of communications in full compliance with EU privacy law. Investigations into serious crimes show that communication apps and web-based services are becoming the preferred mean of communication of criminals in cases involving e.g. terrorism, organised crime, and child exploitation. It is only reasonable that these services be afforded with the same legal basis as ECS for allowing law enforcement access to online communications.

In addition to the above, ETNO would like to remind that the 2001 Council Resolution "on law enforcement operational needs with respect to public telecommunication networks and services" lays out in detail the essential needs of LEAs with regard to legal access to communication data, as a guidance for both Member States and ECS providers. ETNO encourages the EU institutions to develop similar guidelines in respect to law enforcement access to electronic evidence held by ISS providers.

The Cross-Border Dimension

The legal framework for the cooperation between European LEAs and ECS providers also extends to cross-border investigations. Directive 2014/41/EU establishing a European Investigation Order (EIO) has created a single instrument allowing a Member States to gather evidence at the request of another Member State based on mutual recognition. Among others, an EU State's authority can issue an EIO for the interception of telecommunications (i.e., communication content, traffic and location data) to the authority of another country where the subject of the interception is located, requesting for its technical assistance. In case the subject of an approved interception is using the communication address (e.g., phone number or IP address) in another Member State, the intercepting authority will only need to notify its counterpart.

ETNO believes that the EIO represents an adequate mechanism for European LEAs to access electronic evidence held by telecom operators in cross-border investigations. Since the EIO entered into force on May 2017, imposing additional obligations upon ECS providers would be absolutely premature. National authorities and telecom providers still need time to assess the implementation of this new tool and to elaborate findings in regard to its effectiveness.

Furthermore, empowering LEAs to gain direct access to telecommunications data in another Member State would be in stark contradiction with the principles and the rationale of the EIO and would undermine its correct implementation.

In light of the above, ETNO suggests that any new measure to improve cross-border access to e-evidence, if any, be addressed to providers of services other than ECS and that it build on the experience of the EIO. New measures should also be designed to be fully compliant with Directive (EU) 2016/680 on protecting personal data processed for the purpose of criminal law enforcement, which will become applicable as of 6 May 2018.

Directive (EU) 2016/680 should also be considered as the Commission contemplates solutions for direct cooperation between EU LEAs and digital service providers headquartered in third countries. The Directive requires that transfers of personal data to third country authorities only occur if that county has been granted with an "adequacy decision" from the Commission or if appropriate safeguards are in place, with very limited derogations. The Commission and Member States are encouraged to provide international mutual assistance and to develop international cooperation mechanisms to this end. Moreover, the General Data Protection Regulation (EU) 2016/679 (GDPR) that will enter into force on 25 May 2018 specifies that "*[a]ny judgment of a court or tribunal and any decision of an administrative authority of a third country requiring a controller or processor to transfer or disclose personal data may only be recognised or enforceable in any manner if based on an international agreement, such as a mutual legal assistance treaty, in force between the requesting third country and the Union or a Member State.*"

With the above mentioned two legal instruments, the new EU data protection framework highlights the primordial importance of mutual legal assistance treaties (MLATs) and international cooperation mechanisms in underpinning the cross-border exchange of information in the context of criminal investigations. EU law in no way allows foreign countries to mandate that European-based companies transfer e-evidence without the intermediation of the national competent authority. If the EU legislator were to introduce such a duty on service providers established outside of the EU borders, this would raise extraterritoriality jurisdiction issues and risk putting companies in the situation of being forced to comply with EU legislation while breaking another country's law and vice-versa.

Against this background, it is also essential that governments establish fair, accountable and uniform procedures that regulate when and how companies may be compelled by public authorities to provide information in compliance with EU and national rules. Laws must clearly establish the circumstances under which public authorities may issue demands for personal data, the forms that such demands must take, and the specific authorities that are empowered to make them. Companies should be permitted to challenge in courts those demands that are inconsistent with the relevant legal framework. Modern rules that ensure consistent protection of users while providing clear and efficient law enforcement procedures would also benefit the Digital Single Market by discouraging data localisation.

Before concluding, ETNO would like to emphasise that there is no need for a harmonised definition for data exchanged in the context of judicial cooperation. For the purpose of any new legislative initiative on cross-border access to e-evidence, the definitions of personal data in the GDPR and of communication content and metadata in the proposed e-Privacy Regulation are

largely sufficient. For instance, Directive (EU) 2016/680 on data processing for law enforcement purposes does refer to the definition of personal data under the GDPR.

Conclusion

Effective cross-border criminal investigations should be based on clear, efficient mechanisms for cooperation among public authorities. Thorough implementation of EU law and of the available mechanisms for intra-EU cooperation, improvement of MLATs for international cooperation, and expansion of well-established obligations for ECS to cover ISS as appropriate are the way to go. Imposing on service providers additional measures that would expose them to legal uncertainty and potential litigations is not a viable workaround.

ETNO (European Telecommunications Network Operators' Association) represents Europe's telecommunications network operators and is the principal policy group for European e-communications network operators. ETNO's primary purpose is to promote a positive policy environment allowing the EU telecommunications sector to deliver best quality services to consumers and businesses.

For questions and clarifications regarding this position paper, please contact Paolo Grassia, grassia@etno.eu