WE ARE SHAPING THE INTERNET.
YESTERDAY.TODAY.BEYOND TOMORROW.

Additional Remarks on the Public Consultation of the European Commission „On improving cross-border access to electronic evidence in criminal matters“

Berlin/Brussels, 23. October 2017

The European Commission is currently exploring new ways to increase efficiency in cross border investigations in crime, which also addresses the topic of electronic communications, and information (in short e-evidence). While this approach shall relieve burden for Law-Enforcement Agencies (LEAs) and judicial authorities it is questionable whether there is a possible trade-off that may be the compromising of the rule of law. The Commission has launched a public consultation in order to clarify the image of the next steps to be taken on the topic. eco - in addition to the answers already submitted has the following remarks on the topics of the consultation.

- **On Part II: General Questions and Current Situation in your Country / entity**

In Germany, law allows for a broad spectrum of measures for lawful interception of electronic communications and obtaining information on users of phones or devices. These measures are supplemented with safeguards in order to assure that interference with fundamental rights is limited. This legislation has been developed in order to address the possibility that criminals may employ digital services or electronic communications for their activities and refined several times. Hypothesises that employment of digital services obstructs law-enforcement can - at least from a German point of view - negated. The fact that LEAs and judicial authorities have to address local authorities of the respective Member States underlines the rule of law and ensures that legal safeguards deployed are in place and work. This creates certainty for LEAs, judicial authorities, service providers and citizens alike.

Changing this established system brings along several questions which eco has already addressed in its remarks on the Inception Impact Assessment of the e-Evidence Initiative. The guaranteed rights of users of electronic communication and information society services have to be paid respect to. Since a direct access on electronic evidence removes safeguards, which are in place, there is serious concern that their enforcement and guarantee is being delegated to companies, which do not possess the competence and authority to conduct responsibilities of public administrations. Secondly, these measures must be strictly in line with the e-Commerce Directive and its provisions to avoid undermining of the principle of home state regulation and provoke third countries to impose similar rules making compliance with all different rules in the digital world de facto impossible and posing an

immense threat to the digital economy. In addition to that, it would offer potential for confusion with measures already established.

Legal certainty for companies and citizens as well as transparency of intrusive measures and their deployment are elemental for the functioning of a digital single market. Offering new mechanisms to circumvent judicial oversight of member states is problematic. Fostering cooperation and setting standards for measures deployed would be a helpful approach, which would also allow national or local supervisory institutions to harmonize and streamline the processing of access requests.

The central problems for accessing e-Evidence are derived from authorities not being able to comply with different national frameworks or not identifying the location of data itself or the appropriate legal framework. Problems encountered when conducting cross-border requests could be remedied in harmonizing request forms and requested contents allowing national competent authorities to standardize procedures and accelerate the access to relevant information. National frameworks should be revised respectively in order to achieve a common understanding of information to be obtained and should be created where they do not exist yet. These have however to take the protection of the very fundamental rights of European citizens into account as well as the confidentiality of electronic communications as it is already laid down in several national legal frameworks.

- **On Part III: Access to e-evidence by a direct production request/order to the digital service provider**

When taking measures towards lightening access for LEAs and judicial authorities within a European framework, there should be a clear and well-defined red line, which is the home state regulation. The act, which requires investigation, should be punishable in both countries - if not so, this would lead to multiple compliance schemes that cannot be satisfied.

These measures create heavy additional administrative burden for service providers who will possibly have to translate, prove judicially these requests and deploy mechanisms to actually obtain the requested information and transfer it to the respective requesting LEAs - possibly in 28 different ways.

- **On Part IV: Direct access to e-evidence through an information system without any intermediary (e.g. a service provider) involved**

Access to information stored in digital services should be paid respect to the location of the data involved and should not go beyond the data stored on the respective device. There should be no option to circumvent implemented security measures by a service provider (e.g. end-to-end encryption). The protection of fundamental rights and the confidentiality of electronic communications should be paid due respect. The exclusion of a service provider from such measures is hard to

imagine. Notification of at least both service provider and the Members States affected by the measure is mandatory if any legislative measure of this kind is to be further elaborated. eco urgently recommends double checking on whether such a measure can be deployed granting legal certainty for all parties included. Security for and integrity of digital services must be protected at all times in order to keep up the confidence of citizens in these services and their political institutions as the Snowden Incident is dramatically demonstrates.

- **On Part V: International scope**

The main-challenge for LEAs and judicial authorities in requests to access or obtain evidence seems the inability to procure proper requests and their timely processing. Legislation, which would require service providers within the EU and beyond to provide Single Points of Contact, would not provide additional benefits to the schemes established under the MLAT frameworks - especially if LEAs and judicial authorities from all EU Member-States could address their requests towards the respective service providers. The obligation to examine and valuate the requests about their data will take due time and additional efforts, which, in doubt, will not accelerate the processing of the information mentioned but in fact bear the risk that the national service provider will seek clarification before a national court. The problem that exists in the cooperation between the different national LEAs and judicial authorities within their respective legal frameworks will only be relocated to private companies who then are forced to compliance and have to bear the burdens of inappropriate communication between the former. The existing challenges through MLATs will not be met through direct inquiries but through harmonization of legislation and procedures.

eco recommends the review of the existing mechanisms and for creating cross-national structures and mechanisms for investigations as already rudimentarily founded in the European investigation order (Directive 2014/41/EU) which remedy the actual problem of cross-border criminality. Imposing additional burden on communication services and their providers is not helpful.

About eco

eco – Association of the Internet Industry fosters all companies that create economic value with or in the Internet and represents their interests. The association currently represents more than 1,000 member companies.

These include, among others, ISPs (Internet Service Providers), carriers, hardware and software suppliers, content and service providers, and communication companies. eco is the largest national Internet Service Provider association in Europe.