WE ARE SHAPING THE INTERNET.

Association of the Internet Industry e.V.

Key Points:

on the European Commission's Inception Impact Assessment "Improving cross-border access to electronic evidence in criminal cases"

Berlin, 31 August 2017

The European Commission's Inception Impact Assessment (IIA) aims to provide the basis for cross-border access to data and information employed in the context of criminal prosecution. eco – Association of the Internet Industry is monitoring developments in this topic area. eco's members are providers of both telecommunication services and telemedia services. For both sets of providers, a certain dilemma exists: On the one hand, they want to offer high-quality and reliable services whilst guaranteeing their customers secrecy of telecommunications and protection of fundamental rights. On the other hand, where required, they are expected to play a part in fighting serious and organized crime and, increasingly, in combating ordinary crime. While this tension has long proven to be a challenge for providers, for those offering cross-border services, a particular type of challenge is presented by the diverse legal systems in the different Member States.

In this respect, national jurisdictions and territoriality of the law can pose problems for cross-border investigations. The present IIA introduces a wide-ranging set of measures as a possible solution to the enforcement deficit anticipated by the EU Commission in accessing electronic data on a cross-border basis.

The Commission's IIA proposes several options for legislative action in the form of a directive – which does not yet constitute a finalized Commission position:

In the IIA, a legal framework to enable the authorities to issue direct orders to providers in third countries is considered, provided that the evidence in question is handled within the Union's territory. The Commission's IIA proposes two alternatives for the regulation:

- it remains at the discretion of the provider as to whether it complies directly with the order,
- the provider is obligated to comply directly with such an order.

This system considered in the IIA could be augmented by an obligation for service providers located in third countries, but offering services in the EU, to designate a legal representative in the EU for the purposes of the cooperation on the basis of such orders.

The draft also introduces a legal framework enabling law enforcement authorities to access e-evidence without the involvement of the service provider or the owner of the data, via a seized device or an information system. This model could also be considered with respect to data whose storage location is not known or to data which is stored outside of the Union.

Finally, there is also reference to regulations intended to more narrowly define both the types of e-evidence and the operators which fall within the scope of application of the proposed measures.

I. General Preliminary Remarks

eco supports initiatives intended to improve law enforcement on the Internet. However, such initiatives must be proportionate to their application area, for which no details are specified in the present IIA. In the interests of justification vis-à-vis citizens, the degree of the intervention's intensity must also not be disproportionate. The latter is not the case with the present IIA.

From eco's point of view, the following aspects need therefore to be generally guaranteed in the further examination of legislative measures at European level.

- **Constitutionality of the process**
  eco has concerns about the constitutional soundness of the design of a cross-border mechanism for securing electronic evidence. Access to electronic communication and connection data always presents a multiple infringement of fundamental rights, which in Germany is subject to the strict legal requirement of a judicial order. Equivalent security safeguards are often not in place abroad, meaning that, particularly for duty bearers of fundamental rights, a risk of an infringement of fundamental rights exists, or an obligation may exist on providers to cooperate in such an infringement.

- **Sovereign functions should not be transferred to providers**
  A problem identified by eco with the current draft is the fact that the country-of-origin principle of the e-Commerce Directive (Recital 22 and Article 3 of Directive 2000/31/EC) could be undermined, since the regime planned will allow other authorities from EU Member States to directly access the data and information of telecommunications and telemedia services. eco opposes the transfer of sovereign functions to service providers. In this context, improving cooperation on criminal prosecution between law enforcement authorities is deemed to be the more meaningful and sustainable way to enforce the law. Data protection and secrecy of telecommunications must not be eroded. This is not just in the interests of legal certainty for companies who provide trustworthy and reliable services, but also serves the interests of legal certainty for users of such services.

- **Costs for companies must become transparent**

  The IIA proposes two different solutions for handling inquiries from investigating authorities from EU States. In both cases, a guarantee is needed that the considerable personnel and material costs generated for companies by such inquiries remains manageable. As it presently stands, the IIA offers no specifics on legal certainty or on liability issues confronted by companies in processing inquiries.

II. The Proposals in Detail

eco has the following comments to make on the Commission's proposals:

- **Legal framework for cross-border access to electronic evidence**
  Within the context of legislative options, the IIA proposes "a legal framework authorizing authorities to directly request or compel a service provider in another Member State to disclose e-evidence processed in the Union, including appropriate safeguards and conditions". Two variants are also introduced, whereby service providers either are compelled to disclose evidence, or are entrusted to disclose the evidence at their own discretion.

  A direct disclosure of data and information at the request of a foreign authority is problematic. The measures for an obligation to disclose data vary depending on different factors, including the country, applicable criminal legislation, existing security regulations, and administrative structures. However, direct disclosure impinges on the independence of telemedia and telecommunications services. A precisely defined national legal structure, underpinned by security regulations, already exists for these services. Among other instruments, the German Federal Police Office Act (BKA), various state police laws, the G-10 Act, the Telecommunications and Telemedia Act, the German Code of Criminal Procedure, and other ordinances contain precise specifications determining under which framework conditions certain authorities are allowed to access various information systems and data, and stipulating what requirements these authorities must fulfil before accessing data or effecting an order.

  The e-Commerce Directive has moreover also already defined sufficient rules specifying the framework conditions under which data can be released. The existing mechanisms of the Mutual Legal Assistance Treaty (MLAT) and the European Investigation Order in Criminal Matters complement this legislative structure and at the same time ensure that – also abroad – only authorized authorities have access to the relevant information.

If this approach were to be changed, companies would in future have to allocate considerably more resources to the tasks of verifying the legitimacy of inquiries and processing these. A guarantee as it exists within the existing system is consequently no longer available. Instead, companies are being called upon to perform sovereign tasks.

For services providers, there is the additional challenge of having to respond to requests in all official EU languages. This would entail substantial additional costs in terms of human resources, as surplus and permanent capacity would need to be maintained.

What is also unclear is how providers are expected to deal with inquiries that do not constitute a criminal offence in the country in which the service is resident.

Providing details on contact persons for services which are offered within the EU, but whose headquarters are elsewhere, would also prove problematic.

The undermining of constitutional principles is unacceptable, even in the context of criminal prosecution. It would make more sense to improve cross-border cooperation between investigating authorities and thus ensure that investigations run smoothly, rather than burdening companies with sovereign tasks in an area which is sensitive in terms of fundamental rights.

- **Legal framework for access to data and information systems without the involvement of the service provider**

  The IIA also proposes that law enforcement institutions should be able to access possible electronic evidence without the involvement or cooperation of service providers. This measure is viewed critically because, apart from the problems already detailed, it calls the integrity of communication services into question. This is particularly true in the case of access to "seized information systems", which is a very unclear concept in this context. As it appears that such access is expected to occur without notification to national security authorities or service providers, the very feasibility of implementing such a measure is debatable. The intensity of such an intervention casts doubt on the desirability of such a measure from a constitutional point of view. Under any circumstances, it would constitute a serious encroachment on the secrecy of telecommunications, which would not only undermine the confidence of users in digital services, but would also weaken the confidence of service providers in the work of investigation and security authorities. In addition, the extremely vague wording of the passage does not make clear to what extent access to data and information systems can technically occur without the involvement of the service provider, meaning that their involvement is already assumed. eco opposes all measures which move in the direction of

backdoor state activities and the mass groundless collection and storage of communication.

---

eco – Association of the Internet Industry represents the interests and supports all industries involved in generating economic value creation through the Internet. The association currently represents more than 1000 member organizations. Amongst others, these include ISPs (Internet Service Providers), carriers, suppliers of hard and software, content and service providers, and communications companies. This makes eco the largest national association of Internet service providers in Europe.