ITI Promoting Innovation Worldwide

18 November 2019

ITI's proposal for an effective EU e-evidence framework

Executive Summary

- Cross-border data access request obligations under the proposed e-evidence framework need to provide sufficient **safeguards for fundamental rights of users**. While the EU's data protection framework provides rules and exceptions for compliance with legal obligations like requests to access to data by law enforcement authorities, we caution that with the broadening of data access requests needs to come a broadening of mechanisms to ensure due process and individual guarantees that exist in the context of national legal systems.
- **Scope:** For this purpose, we urge policymakers to include a **catalogue of criminal offences that would clearly limit the scope of EPOCs and EPOC-PRs**.
- **Dispute mechanisms:** Service providers should not be entangled in disputes between national enforcement authorities – the proposal should in particular:
    - Preserve **avenues for both enforcing states and service providers to challenge the validity of EPOCs and EPOC-PRs**.
    - Extend the **grounds for service providers to challenge EPOCs and EPOC-PRs to include violations of the EU Charter of Fundamental Rights**.
- **International cooperation:** International systems diverge and a conflict of law between the EU's e-evidence framework and third countries' provisions on blocking statues is bound to occur; the EU should ensure that the e-evidence proposal outlines a **clear procedure in case of conflict of law with third countries**.
- **Preservation timelines:** Non-renewable preservation deadlines may prompt unnecessary EPOCs if authorities fear losing data. Such precipitative decisions threaten fundamental rights of users for no good reason. We advocate for the **introduction of limited extension options for EPOC-PRs that allow for more time to investigate before issuing an EPOC, while avoiding becoming an open-ended data retention tool.**
- **Gag-orders:** In order to fulfill obligations towards users, we strongly urge policymakers to clarify provisions on confidentiality and user information in order to ensure **clear limits to cases in which users cannot be informed of law enforcement authorities seeking access to their data**.
- **Penalties:** Fines could have the effect of dissuading companies from assessing the lawfulness of a data request in order to avoid sanctions. To avoid such a scenario, we urge policymakers to reassess critical elements of the proposal and **introduce appropriate ways for service providers to challenge requests**.
- **Response times:** While our members are committed to support investigations in a timely manner, **urgency shall not come at the expense of thorough assessment of a data access request**. We support an extension of the **deadline for emergency cases to 24 hours** in order to provide sufficient time to evaluate a request and comply.
- **Timely adoption:** As we see the emergence of unilateral action by EU Member States, we urge policymakers to make the conclusion of this file a priority in order to **avoid legal uncertainty for all actors involved**.

Background

- On 17 April 2018, the European Commission unveiled two proposals: a draft Regulation on cross-border access to and preservation of electronic data held by service providers and a draft Directive to require service providers to appoint a legal representative within the EU. The envisaged regulation would create two new instruments: a

Global Headquarters
700 K Street NW, Suite 600
Washington, D.C. 20001, USA
+1 202-737-8888

Europe Office
Rue de la Loi 227
Brussels - 1040, Belgium
+32 (0)2-321-10-90

info@itic.org
www.itic.org
@iti_techtweets

European Production Order (EPOC) asking service providers to produce e-evidence in form of access data, transactional data, subscriber data or content data and a European Preservation Order (EPOC-PR) asking them to preserve this evidence for a set period of time.

- The core of the Commission's "e-evidence" initiative is that national judicial or administrative bodies can ask service providers to produce and to preserve data for the investigation or prosecution of a crime. To date, national judicial authorities receive and authorize foreign requests on a case-by-case basis to ensure lawfulness of requests.
- The Council of EU Member States has meanwhile also published its General Approach in November 2018, significantly reducing fundamental rights safeguards in the Commission's proposal and expanding rights for issuing authorities/states.
- The European Parliament's Civil Liberties Committee (LIBE) under the lead of Member of the European Parliament (MEP) Birgit Sippel, has published its draft report on 8 November (referred to as "the draft EP report" henceforth). It introduces crucial safeguards for fundamental rights and reduces liability for service providers, while boosting rights for enforcing authorities to challenge EPOs. The draft EP report needs to be approved by the full LIBE Committee and subsequently the full European Parliament.

ITI Recommendations for a balanced e-evidence sharing framework

In order to develop a European framework that facilitates criminal investigations while protecting individuals' rights, ITI would like to put forward the following thoughts and recommendations taking into account the General Approach of the Council published on 11 June 2019 and the draft EP report of 8 November.

- **Scope of EPOC and EPOC-PR:** There is a risk that EPOCs and EPOC-PRs could be used by enforcing states to request data that would otherwise not be disclosed as the offence committed in the issuing state is not a criminal offence in the framework of this Regulation in the enforcing state. In order to avoid such a situation, the grounds for law enforcement to request preservation of all kinds of data and production of access data need to be clarified. Proportionality of the request and a similar domestic order being available for the same criminal offence in the issuing state are the criteria indicated by the Commission and Council texts. These criteria are a good start but do not go far enough to safeguard fundamental rights. Transactional and content data requests are limited to criminal offences with a 3-year maximum sentence in both the Commission and Council's texts; while this would for example exclude criminal offences like slander, defamation or libel in some Member States, there is no guarantee that similar offences would be excluded in other EU countries, since punishment of criminal offences is a matter of national competence not harmonized at EU level.
  We endorse the draft EP report's suggestion to include a catalogue of criminal offences that would clearly limit the scope of EPOCs and EPOC-PRs (Amendment 267 Annex 3a). We agree with the need for a list that includes major crimes like terrorism, murder and child sexual abuse while clearly excluding less serious offences such as slander, defamation or libel. We recommend clarification on some of the listed offences, such as on what "computer-related crimes" would concretely entail. We support the elevation of the definition of serious crimes from 3 years to 5 years. We also appreciate additional safeguards made to protect fundamental rights by the draft EP report, including clear references to the EU's Charter of Fundamental Rights (Amendments 11, 13).

- **Dispute mechanisms for enforcing authorities:** The procedures in the draft Regulation vest the power to launch an assessment of the legality of a request mainly with the issuing authority, placing a disproportionate burden on the service providers that are involved in the fulfilment of such requests. While companies are committed to aiding criminal investigations and safeguarding fundamental rights, service providers are not always best placed to perform validity assessments for EPOCs and EPOC-PRs. The Council's addition of important rights for the enforcing state to assess the legality of EPOCs for content data is a step in the right direction but does not go far enough. **We believe the enforcing authority should be informed of (but not request authorization for) an issuing authorities' EPOCs and EPOC-PRs in a timely manner; this is in line with the draft EP report's suggestion**

that EPOs should be sent simultaneously to service providers and enforcing authorities (Amendment 127) and that the latter be granted a 10-day period to object to an EPO (Amendment 142). The enforcing authority should also be able to challenge EPOCs and EPOC-PRs directly, and we applaud the addition of a catalogue of grounds for non-recognition or non-execution for enforcing authorities suggested by the draft EP report (Amendment 161).

- **Dispute mechanism for service providers:** Grounds on which service providers can challenge EPOs diverge between Commission proposal, Council text and European Parliament. The Council text for example removes grounds based on fundamental rights abuses, or in cases in which EPOs are incomplete, contain manifest errors or do not provide sufficient information. The Council also puts significant responsibilities on service providers e.g. in cases where service providers serve as a gatekeeper to the enforcing states' authority to refuse to enforce an EPOC or EPOC-PR (Art. 14). In this case, the enforcing state can only exercise its right to refusal if the service provider also refuses to comply with the EPOC or EPOC-PR; the enforcing state may not even be made aware of the case in instances where service providers produce an EPOC or EPOC-PR and don't challenge the request. This situation puts disproportionate burden on service providers, who often don't have the capacity to conduct assessments on the validity of an EPOC or EPOC-PR. **Service providers should therefore also be able to challenge EPOCs and EPOC-PRs based on clearly defined grounds including procedural aspects but also concerns in relation to fundamental rights as outlined in the EU Charter of Fundamental Rights. We strongly object to the Council's deletion of references to the EU Charter of Fundamental Rights in Article 14 (4) and (5). We urge policymakers to adopt the EP draft report's suggested dispute mechanism and grounds for objection to an EPO; we would further suggest an extension of the right to challenge EPOs for service providers on the same grounds as those afforded to enforcing authorities. In cases where a service provider challenges an EPOC or EPOC-PR, deadlines also need to be paused in order to ensure a proper assessment of the situation.**

- **International cooperation:** Service providers will risk significant consequences in cases where there is a conflict of law between the EU's e-evidence framework and third countries' regimes if the legal text does not outline appropriate review mechanisms. We welcome efforts to create a harmonized international framework for e-evidence sharing in criminal investigations in order to create legal certainty for all actors involved and welcome the European Commission launching negotiations with the United States in this context. However, we fear that a conflict of law between third countries and the EU is ahead if the proposed Regulation does not clarify procedures in cases of conflict of law with third countries. Many countries have so-called blocking statues in place: a system that forbids service providers to disclose data to third countries. For example, the US Stored Communications Act (SCA) is a blocking statute that prohibits US-based providers from turning over the content of communications to foreign governments. The new e-evidence framework would allow for extra-territorial reach, requiring production of evidence in cases involving third countries, while those countries with blocking statues would conflict with the framework. While the Commission text had included clarification on this point, the Council's text downgrades the review mechanisms by deleting article 15 which provided for a mechanism in which third countries could exercise their protective functions in relation to human rights and/or state interests by preventing the execution of an EPO under certain conditions. In addition, the possibility for third countries to object an EPO is a departure from the Cloud Act mechanism. With the deletion, the Council has significantly reduced the influence that authorities in third countries can have in the process, which was criticized by the European Data Protection Board (EDPB). The failure to provide for sufficient review mechanisms in cases of conflict of law could compel service providers to execute requests despite them conflicting with the laws of a third country. **We therefore endorse clarification on the review procedure in cases of conflict of law with third countries as brought by the draft EP report's suggestion for a process involving the enforcing authority and including a clear deadline of 10 days to assess potential conflicts (Amendments Am 64, 65, 67, 68 & 173). We encourage the co-regulators to accept this addition.**

- **Preservation timelines:** The current Council text and the Commission proposal both propose a preservation period of 60 days in cases where service providers receive an EPOC-PR. While this seems like a long time, we caution that the expiry of the 60 days deadline may prompt unnecessary EPOCs if authorities fear losing data after this time frame. Such precipitative decisions threaten fundamental rights of users for no good reason. The

draft EP report suggests an initial 10-day preservation timeline (during which enforcing authorities can also challenge the validity of an EPOC-PR). This timeline is followed by a potential 30-day preservation period that can be renewed once for another 30 days; this is in line with preservation timelines on European Investigation Orders. The full process would therefore increase maximum preservation time to 70 days (Amendments 50, 152-154). **We welcome this process and the introduction of additional "checkpoints" for authorities to reconsider the necessity for service providers to preserve data. The new process and ability to renew the preservation time will be beneficial to all actors involved, providing more time to law enforcement authorities to investigate, while protecting fundamental rights of citizens and avoiding unnecessary burden on businesses.**

» **Gag-orders and user rights:** In case of gag orders, an authority can forbid a company from disclosing to an individual that a request for their data was made as part of a criminal investigation. Gag orders create tensions with the EU Charter of Fundamental Rights. Since companies have to carefully balance obligations towards their users and law enforcement requests, we support the Commission's original approach allowing service providers to inform users of access requests unless told otherwise by issuing authorities. The Council text reverses this situation, prescribing that service providers "shall only inform the person whose data are being sought if explicitly requested by the issuing authority" (Art. 11 (1)). The Council further opens a loophole in paragraph (2) allowing authorities to "delay informing the person whose data were sought as long as it constitutes a necessary and proportionate measure", which means authorities could delay this information endlessly. To even strengthen this provision, paragraph (3) further details that in cases where more than one person's data were disclosed in an investigation, the authorities may fully refrain from informing the data subject if they decide that the interests of the other affected individual outweigh the primary data subject's. These two provisions open the door for a non-transparent system in which holding local law enforcement accountable becomes more difficult. The draft EP report has mitigated this by requiring that "'gag rule' should only be an exception to the general rule" and has made important clarifications on this point (Amendment 163-165). **We therefore strongly urge policymakers to accept the insertion of language proposed in the draft EP report on confidentiality and user information in Article 11 that ensures that users may not be informed of law enforcement authorities seeking access to their data only in a very limited number of cases, for a limited time and only based on a court order. However, we suggest the additional clarification that once the ban is lifted, not only must the Member States inform users, but also service providers should be allowed to do the same.**

» **Penalties:** The Council text introduces a reference to pecuniary sanctions of up to 2% of total worldwide annual turnover to be imposed on service providers that fail to comply with an EPOC or EPOC-PR. This fine does not meet the requirements of it being "proportionate, effective and dissuasive". Service providers have an interest in facilitating criminal investigations for the benefit of the societies that they serve and to protect users from harm e.g. in cases of imminent terrorist threat. Should they decide to deny a data access request, they would in most cases do so in order to avoid what they believe to be a manifest infringement of fundamental rights outlined by the EU Charter of Fundamental Rights. A fine would not change this decision. We applaud the draft EP report for recognizing this mismatch and consequentially removing strictly defined pecuniary sanctions from the text. **We urge policymakers to reassess critical elements of the proposal and introduce appropriate ways for service providers to challenge EPOCs and EPOC-PRs rather than introducing financial penalties that could disincentivize companies from assessing the lawfulness of a data request. The national level is best suited to determine sanctions as proportionality would depend on sanctions for other criminal offences in a given EU country.**

» **Response times:** With merely 6 hours response time, timelines suggested by both the Council and the Commission are very tight in order to make a proper assessment of a request and to assess the need for action. The draft EP report suggests a more reasonable timeframe for responses of 24 hours in emergency cases. While urgency is key in emergency situations, it should not come at the expense of due diligence. **We suggest that the timeline for emergency cases be raised to 24 hours, as per the draft EP report's suggestion (Amendment 47, 144, 145, 205), in order to provide sufficient time to evaluate a request and comply.**

About us - ITI is the global voice of the tech sector. We advocate for public policies that advance innovation, open markets, and enable the transformational opportunities that our companies are creating. Our members represent the entire spectrum of technology: from internet companies, to hardware and networking equipment manufacturers, to software developers. ITI's diverse membership and staff provide a broad perspective and insight on policy activities around the world.

For more information and inquiries, please contact Guido Lobrano globrano@itic.org and Vivien Zuzok vzuzok@itic.org - +32 2321 10 93