ITI Promoting Innovation Worldwide

11 February 2020

ITI Recommendations on LIBE Committee Amendments for Compromise

Draft e-Evidence Regulation (2018/0108(COD))

Topic	Explanation	Our Recommendation
Scope of the Regulation: List of Crimes rather than Penalty-based approach	There is a risk that European Production Orders (EPO) or European Preservation Order (EPO-PR) 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 European 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 European 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. As pointed out by amendment 324, a 3-year maximum sentence threshold does not cover offences such as possession of child pornography in France. This illustrates that rigid time-based thresholds are not useful in pursuing serious crimes across Member States with no common definition of what constitutes a serious crime. We believe that a clear list of criminal offences including possession and/or distribution of child pornography would solve this problem.	We therefore support the **insertion of a list of serious crimes** covered by this legislation as proposed by Rapporteur Birgit Sippel in her draft report and in amendments (Amendment 660). This list should include for example **sexual exploitation of children and child pornography, terrorism** and **murder** as serious crimes. A list of criminal offences is proportionate to reach the goals of the Regulation without broadening the scope of the law (to cover for example slander or libel). This would safeguard fundamental rights without creating unsurmountable administrative burden for law enforcement authorities and service providers alike.

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

Scope of the Regulation: Exclusive Means	We support a rule that prohibits national authorities from using domestic procedures in cases that fall within the scope of this Regulation. Article 1(2) of the European Commission proposal states that the Regulation is "*without prejudice to the powers of national authorities to compel service providers established or represented on their territory to comply with similar national measures*." There is a risk that Member States may read this as allowing them to use domestic legal processes to compel disclosure of data on a cross-border basis. We caution that this may threaten fundamental rights of users if domestic procedures contain fewer safeguards than the proposed EU Regulation. In addition, government requests for data production or preservation should only be issued pursuant to judicial oversight such as a warrant, subpoena or other court order from the Issuing State. "*Any other competent authority as defined by the issuing State*" as provided in Article 4.1 (a) broadens the list of competent authorities too much.	We call upon policymakers to support Amendments 393 (Lagodinsky), 394 (Ernst), 782 (Ernst) for compromise.
Safe Harbor for Service Providers	Recital 46 of the European Commission's proposal states that, "*[n]otwithstanding their data protection obligations, service providers should not be held liable in Member States for prejudice to their users or third parties exclusively resulting from good faith compliance with*" an EPO or EPO-PR. The meaning of the phrase "notwithstanding their data protection obligations" is unclear, and the operative provisions of the European Commission's proposal do not include any analogous safe harbour from liability for service providers. We believe the future framework should grant service providers a stronger safe harbour from liability for consequences from "good faith" compliance with the Regulation.	We call upon policymakers to support Amendments 365 (Lagodinsky) and 705 (Lagodinsky) for compromise.
Dispute mechanism for service providers	Grounds on which service providers can challenge EPOs diverge between European 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 EPO (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 EPO; the enforcing state may not even be made aware of the case in instances where service providers produce an EPO and don't challenge the request. This situation puts disproportionate burden on service providers. Policymakers should therefore preserve avenues for both enforcing states and service providers to challenge the validity of EPOs 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 object to the Council's deletion of references to the EU Charter of Fundamental Rights in Article 14 (4) and (5). We also call for a careful reconfiguration of response timelines for service providers in the European Parliament's future text. An enforcing authority can theoretically object to an EPO until the last minute of the 10-day deadline, creating legal uncertainty for service providers who are seeking to comply with EPOs in	We call upon policymakers to support Amendments 141-148 (Sippel), 583 (Sippel et al.), 590 (Lagodinsky), 593 (Lagodinsky), 596 (Ernst), 608 (Körner et al.), 624 (Körner et al.), 643 (Körner et al.) and 649 (Ernst), 600 (Ernst), 601 (Lagodinsky), 606 (Lagodinsky), 610 (Lagodinsky), 619 (Ernst) for compromise.

	a timely manner. Under the proposed system, service providers would be faced with legal uncertainty should they respond before the last minute of the response deadline, as the enforcing authority could still raise an objection until this point. In summary, we encourage policymakers to adopt the European Parliament 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 while also adjusting response timelines for enforcing authorities and service providers.	
Encrypted data	Data requests under this legal instrument should not require a provider to weaken the security of its technology, introduce vulnerabilities or disclose confidential business information or proprietary technology. Service providers should therefore not be obliged to provide keys for encrypted data under this Regulation. General and indiscriminate data retention and limitations on encryption and security must be avoided in order to protect user privacy.	We call upon policymakers to support Amendment 398 (Körner et al.)
Preservation timelines	The current Council text and the European 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 European Parliament 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.	We call upon policymakers to support Amendment 638 and 628 (Ernst), Amendment 636 (Kaljurand, Moraes), Amendment 635 (Lagodinsky) for compromise.
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 European 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*	We call upon policymakers to support Amendments 672 (Ernst), 674 (Kaljurand et al.), 675 (in't Veld), 676 (Ernst), 677 (Kaljurand et al.) 678 (in't Veld),

	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 European Parliament 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 European Parliament 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. In addition, there should be more precision as to available means for service providers challenging the non-disclosure 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.	681 (Ernst) and 687 (Ernst) for compromise.
Response time	With 6 hours response time for emergency cases, the timelines suggested by both the Council and the European Commission are very tight in order to make a proper assessment of a request and to assess the need for action and proceed accordingly. Technical circumstances, such as access restrictions for example in cases where data is stored in a decentralised way via Infrastructure as a Service ("IaaS") providers, need to also be considered. In such cases, gaining access to stored data may require a more complex process that could jeopardise the ability of service providers to respond immediately in emergencies. Where it is not possible to provide the information in the requested time, the information may be provided in phases without undue further delay. While urgency is key in emergency situations, it should not come at the expense of due diligence and needs to factor in technical possibilities. We suggest that the timeline for emergency cases be raised to 24 hours in order to provide sufficient time to evaluate a request and comply.	We call upon policymakers to support Amendment 346 (Sippel et al), 348 (Lagodinsky), Amendment 460 (Körner et al.) and Amendment 610 (Lagodinsky) for compromise.