Public Consultation on improving cross-border access to electronic evidence

BSA | The Software Alliance's supplemental position paper

October 2017

BSA | The Software Alliance ("BSA")[1], the leading advocate for the global software industry, welcomes the opportunity to provide additional views to the European Commission's public consultation on "improving cross-border access to electronic evidence in criminal matters". BSA supports the efforts of the European Commission to address the challenges facing cross-border access requests for electronic evidence ("e-Evidence") and shares the desire to achieve greater harmonisation and legal certainty for citizens, national authorities and digital service providers.

We believe the European Commission should seek to create a future legal framework that builds upon the provisions of the European Investigation Order ("EIO")[2], which effectively provides assistance between law enforcement and judicial authorities in different Member States. The future legal framework should complement the EIO by creating a set of clear and coherent principles to enable requests by law enforcement and judicial authorities in one Member State to be made directly to a service provider in another Member State for the disclosure of data stored within the EU.

As the European Commission continues to evaluate its future legislation, we would like to bring to your attention the following issue-specific points:

1. **Legal Basis & Mutual Recognition** – The principle of mutual recognition should constitute the foundation of any future legal instrument. Any proposal should seek to reduce jurisdictional conflicts within the EU and enhance the efficiency of issuing and responding to lawful cross-border requests.

2. **Investigative Measures & Jurisdiction** – The proposal should create the ability for law enforcement agencies to issue "production requests" (leaving to the discretion of the service provider a decision on whether to provide a response) and "production orders" (an obligation on service providers to respond).

---

[1] *BSA | The Software Alliance (www.bsa.org) is the leading advocate for the global software industry before governments and in the internationals marketplace. Its members are among the world's most innovative companies, creating software solutions that spark the economy and improve modern life. With headquarters in Washington, DC, and operations in more than 60 countries, BSA pioneers compliance programs that promote legal software use and advocates for public policies that foster technology innovation and drive growth in the digital economy.*
BSA's members include: Adobe, ANSYS, Apple, Autodesk, Bentley Systems, CA Technologies, CNC/Mastercam, DataStax, DocuSign, IBM, Intel, Intuit, Microsoft, Oracle, salesforce.com, SAS Institute, Siemens PLM Software, Splunk, Symantec, The MathWorks, Tend Micro, Trimble Solutions Corporation, and Workday.

[2] *Directive 2014/41/EU "Regarding the European Investigation Order in Criminal Matters"*

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

3. **Applicable Data** – The future legal framework should be applicable to traffic data, subscriber data and content data, subject to appropriate limitations and safeguards. It should set out a harmonised definition of the data exchanged, including in the context of judicial cooperation, and creating a clear hierarchy between each category of data in terms of the extent to which they interfere with an individual's privacy. If a harmonized standard for accessing content cannot be achieved across Member States, the future legal framework should apply only to metadata.

4. **Territoriality** – Any future legal framework should avoid creating conflicts of law. The territorial scope of any new investigative measures should be limited to data stored by a service provider within the EU, as data stored outside of the EU may be subject to legal frameworks that conflict with those of the EU.

5. **Recipient of Investigative Measure** – The future legal framework should require requesting law enforcement agencies to direct investigatory measures solely to the "main establishment" of the service provider. Only entities acting as "data controllers" should be the recipients of an investigative measure as they are legally responsible for the management of their data.

6. **Exigent Circumstances** – It will be important for the future legal framework to include a special procedure for responding to requests issued under "exigent circumstances," in which swift action is required to avoid death or physical injury of a person or persons. Under such circumstances, service providers should be able to responds to investigative requests without meeting all the safeguards laid out in the legal framework.

7. **Derogations** – The proposal should include recognition of the existence of circumstances where a service provider is unable to comply with an investigative measure. Such situations include instances where the service provider does not hold the requested data or cannot identify the subscriber.

8. **Transparency & Notification** – The framework should allow for notification by a digital service provider to any subscriber whose data is targeted by an investigative measure.

9. **Liability** – The future legal framework should clearly state that digital service providers should not be liable for disclosing data to a Member State law enforcement authority following the receipt of an investigative measure.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

Issues and BSA Positions

1. Legal Basis & Mutual Recognition

BSA believes that the principle of mutual recognition should constitute the foundation of any future legal instrument. Any proposal should seek to reduce jurisdictional conflicts within the EU and enhance the efficiency of issuing and responding to lawful cross-border requests. We therefore encourage the European Commission to select Article 82 of the Treaty of the Functioning of the European Union ("TFEU") as the legal basis for any future legislation.

This will require all EU Member States to provide recognition to a law enforcement agency in another Member State, which has obtained relevant domestic authorisation to request data from a service provider established in another Member State. Recipient digital service providers will consequently have the same obligations to comply with any request as if it were issued by the law enforcement agency of its main establishment.

The European Commission should seek to replicate the provisions of the EIO whereby the law enforcement agency in the issuing Member State is obligated to assess whether the evidence being sought is necessary and proportionate for the purposes of the investigation.

To avoid the erosion of trust amongst citizens, the future legal framework should also ensure that a law enforcement authority effectively demonstrates that the investigative measure and evidence being sought ensure the full respect for the EU Charter of Fundamental Rights ("CFREU"). Any limitation of such rights would need to meet the strict proportionality and necessity requirements as set out in Article 52 CFREU.

2. Investigative Measures & Jurisdiction

When considering the investigative measures to be introduced by the future legal framework, we believe the proposal should create the ability for law enforcement agencies to issue "production requests" (leaving to the discretion of the service provider a decision on whether to provide a response) and "production orders" (an obligation on service providers to respond).

BSA recognises that the use of such investigative measures, particularly "production orders", represents a departure from standard criminal investigative procedure in most Member States and may lead to questions of jurisdiction. We therefore encourage the future legal framework to clarify that such measures should only be triggered where the investigated conduct is recognised as a "serious" criminal offense. We believe that the introduction of a minimum threshold defining the applicable offenses could achieve this goal. The listing of such applicable offenses could build upon those set out in Annex D of the EIO. In instances where jurisdiction could be claimed by more than one Member State, we believe that conflicts could be resolved in accordance to the procedures set out in Framework Decision 2009/948/JHA.

Regarding the "jurisdictional trigger" for enabling a request, the framework should cover service providers "offering services" in the Member State of the requesting law enforcement authority. This is consistent with the Council of Europe Budapest Convention on Cybercrime ("CoE Convention")[3].

3. Applicable Data

BSA recognises that various definitions exist for data generated and processed by digital service providers that are of interest to Member State law enforcement authorities. These include "subscriber information" as set out in the CoE Convention, "traffic data" and "location data" as set out in current ePrivacy Directive[4], and "electronic communications metadata" and "electronic communications content" as set out in the draft ePrivacy Regulation. We believe that the future legislation would benefit from a harmonised definition of the data exchanged in the context of judicial cooperation, while setting out a clear hierarchy between each category of data in terms of the extent to which they interfere with an individual's privacy.

To ensure legal clarity, BSA believes that the future legal framework should be applicable to traffic data, subscriber data and content data, subject to appropriate limitations and safeguards. If a harmonized standard for accessing content cannot be achieved across Member States, the future legal framework should apply only to metadata. Digital service providers should only be required to produce data generated or processed in the course of supplying their service and should not be required to disclose or generate data that their service would not normally produce.

4. Territoriality

Any future legal framework should avoid creating conflicts of law. We encourage the European Commission to limit the territorial scope of any new investigative measures to data stored by a service provider within the EU, as data stored outside the EU may be subject to legal frameworks that conflict with those of the EU. Such a scope would be consistent with the approach of the General Data Protection Regulation ("GDPR")[5], particularly Article 48, which limits claims of extraterritorial jurisdiction by third country states seeking data stored within the EU.

The European Commission should instead seek to find common reciprocal solutions with international partners so that service providers operating across numerous jurisdictions are not faced with conflicting legal obligations. We believe that a dedicated dialogue with third countries should be immediately pursued. An intra-EU framework must be complemented with durable international frameworks.

When considering the trans-Atlantic context, we believe the recent introduction of the International Communications Privacy Act ("ICPA") in the U.S. provides a unique opportunity for

[3] *Article 18(1)(b) – 23.XI.2001*
[4] *Directive 2002/58/EC*
[5] *Regulation (EU) 2016/679 on the "protection of natural persons with regard to the processing of personal data and on the free movement of such data*

the creation of a EU-U.S. framework supplementing the more laborious mutual legal assistance treaty ("MLAT") process.

5. Recipient of Investigative Measure

Only entities acting as "data controllers" should be the recipients of an investigative measure as they are legally responsible for the management of their data. When a law enforcement authority would find it impossible or inappropriate to direct the request to the "data controller", the investigative measure should only be directed to the service provider with whom the subscriber has an apparent direct contractual relationship (i.e. "data processor") under exceptional and clearly defined circumstances.

We wish to note that digital services may compromise of numerous layers, operated by different entities, using shared resources with various degrees of transparency as to the data generated by data subjects utilising the service. It is important to minimise the risk of interference and intrusion resulting from investigative measures being sent to upstream service providers who may not have a direct contractual relationship with the subscriber. Under such situations, a service provider should be able to ask for redirection of a request to any downstream service provider.

6. Exigent Circumstances

It will be important for the future legal framework to include a special procedure for responding to requests issued under "exigent circumstances". BSA envisages such situations to include imminent threat to life, and danger related to potential for serious physical injury of a person or persons. The European Commission should explore utilising language in the GDPR related to the "vital interests of the data subject". Under such circumstances, service providers should be able to responds to investigative requests without meeting all the safeguards laid out in the legal framework.

7. Derogations

BSA believes that the proposal should include recognition of the existence of circumstances where a service provider is unable to comply with an investigative measure. We envisage such situations to include instances where the service provider does not hold the requested data or cannot identify the subscriber. Such circumstances could build upon those found in Article 11 of the EIO.

Furthermore, the future legal framework should note that a service provider may be prohibited from data disclosure due to a conflicting Member State legal obligation or compliance request by a domestic law enforcement authority.

Avenue des Arts 44
1040 Brussels
Belgium

P +32 (0)2 274 13 10
W bsa.org
EU Register of Interest Representatives 75039383277-48

8. Transparency & Notification

When considering transparency, the future legal framework should allow for notification by a digital service provider to a data subject targeted by an investigative measure. This is consistent with the recent Court of Justice of the European Union ("CJEU") jurisprudence.[6] We believe that the future framework should allowed service providers to provide prior notification to a data subject before the disclosure of data to a law enforcement authority resulting from an investigative measure, subject to appropriate limitations.

BSA recognises that in some cases notification should be avoided due to the investigation being potentially jeopardised. The future legal framework should set out a clear list of circumstances whereby prior notification to the data subject is not allowed. The investigative measures should expressly state to the digital service provider that prior notification is impermissible and the issuing Member State law enforcement authority should be obliged to notify the service provider when post notification to the data subject would be permissible.

9. Liability

BSA believes that the future legal framework should clearly state that digital service providers should not be liable for disclosing data to a Member State law enforcement authority following the receipt of an investigative measure. Conversely, service providers should not be liable for refusing to disclose data to a Member State law enforcement authority following the receipt of an investigative measure, where one of the derogations is exercised.

* * *

For further information, please contact:
Thomas Boué, Director General, Policy – EMEA
thomasb@bsa.org or +32.2.274.13.15

[6] *Tele2 Sverige AB (C-203/15)*