PRIVACY INTERNATIONAL

Privacy International's response to the European Commission's public consultation on improving cross-border access to electronic evidence in criminal matters

25 October 2017

Public consultation on improving cross-border access to electronic evidence in criminal matters

Fields marked with * are mandatory.

Introduction

Obstacles to accessing electronic evidence complicate criminal investigations and therefore affect criminal justice in the digital age. Criminal procedural measures to gather evidence as part of a criminal investigation are usually national in scope. By contrast, obtaining electronic evidence frequently has cross-border implications. Therefore, authorities have to rely on judicial cooperation mechanisms like mutual legal assistance (MLA) or, within the EU, mutual recognition, on the direct cooperation of service providers, or on direct access to obtain electronic information. All three channels raise different types of issues affecting the investigations that may result in abandoned and unsuccessful cases and, ultimately, in a less effective criminal justice.

In the perspective of improving access to electronic evidence in criminal investigations, the Commission will assess the scope for horizontal or further sectorial action at EU level, while respecting the principle of subsidiarity. The present public consultation is intended to feed this assessment - without, however, either prejudging any action by the European Union or prejudging the legal feasibility of an EU action with regards to the limits of the Union's competence.

About you

1 You are welcome to answer the questionnaire in any of the 24 official languages of the EU. Please let us know in which language you are replying.

English

*2 You are replying

- ○ as an individual in your personal capacity
- ◉ in your professional capacity or on behalf of an organisation

*11 Respondent's first name

Tomaso

*12 Respondent's last name

Falchetta

*13 Name of the organisation

Privacy International

*14 Email address

tomasof@privacyinternationa.org

*15 What is the nature of your organisation?

Please select the answer option that fits best.

- Electronic communication service provider (e.g. telecommunications operators, transmission services excluding broadcasting, etc.)
- Information society service provider (e.g. online services, cloud services, social networks, platforms, etc.)
- Professional/business association
- Government of a Member State or regional government
- Law enforcement or judicial authority or public authority directly related to it (e.g. Ministry of Justice, Ministry of Interior)
- Other public authority/administration
- EU institutions or agencies
- Data protection authority
- Academic/research institution
- Law firm
- (●) Non-governmental organisation (NGO)
- Other

*17 Is your organisation included in the Transparency Register?

If your organisation is not registered, we invite you to register here, although it is not compulsory to be registered to reply to this consultation. Why a transparency register?

- (●) Yes
- No
- Not applicable

*18 If so, please indicate your Register ID number.

78180074927-85

*19 Place of establishment (main headquarters in case of multinational organisations)

- Austria
-

Belgium
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland
- France
- Germany
- Greece
- Hungary
- Ireland
- Italy
- Latvia
- Lithuania
- Luxembourg
- Malta
- Netherlands
- Poland
- Portugal
- Romania
- Slovak Republic
- Slovenia
- Spain
- Sweden
- (●) United Kingdom
- Other

*21 Your contribution,

Note that, whatever option chosen, your answers may be subject to a request for public access to documents under Regulation (EC) N°1049/2001

- (●) **can be published with your organisation's information** (I consent the publication of all information in my contribution in whole or in part including the name of my organisation, and I declare that nothing within my response is unlawful or would infringe the rights of any third party in a manner that would prevent publication)
- ( ) **can be published provided that your organisation remains anonymous** (I consent to the publication of any information in my contribution in whole or in part (which may include quotes or opinions I express) provided that it is done anonymously. I declare that nothing within my response is unlawful or would infringe the rights of any third party in a manner that would prevent the publication.

Part II: General Questions and Current Situation in your country/entity

The *use of electronic communication tools is constantly growing, so are the criminal investigations that require electronic evidence*

*22 Instead of using landline and meeting in person criminals use more and more other information society services, such as social media, webmail, messaging services and apps to communicate. Do you consider the increased use of information society services as an obstacle for effective criminal investigations?

- ○ Yes
- ◉ No
- ○ No opinion

*24 In cross-border cases law enforcement and judicial authorities regularly have to address a judicial authority of another State via a judicial cooperation mechanism such as mutual legal assistance or EU mutual recognition mechanisms. Do you believe direct cross-border cooperation of law enforcement and judicial authorities with digital service providers will bring an added value in criminal investigations?

- ○ Yes
- ◉ No
- ○ No opinion

*26 Should the European Commission propose measures to improve direct cooperation of EU law enforcement and judicial authorities with digital service providers headquartered in third countries under the condition that sufficient safeguards are in place to protect your fundamental rights?

- ○ Yes
- ◉ No
- ○ No opinion

27 Which concerns would an EU initiative in the area of electronic evidence raise in your view?

	Very relevant	Relevant	Somewhat relevant	Not relevant	No opinion
*Negative impact on (fundamental) rights guaranteed by national law / EU Law	◉	○	○	○	○
*Loss of sovereignty for your Member State	○	○	◉	○	○
*Risk that third countries impose similar obligations to service providers to disclose electronic evidence stored in the EU (reciprocity)	◉	○	○	○	○

30 Others/comments (please use the space below)

500 character(s) maximum

Irrespective of the way data (subscriber information, metadata, content) stored extraterritorially is accessed (e.g. MLAT, mutual recognition regimes, police-to-police cooperation or direct request by the national authorities to service providers in another country) the following principles and safeguards (based on international human rights law) must apply: legality, necessity and proportionality, prior judicial authorisation, effective oversight, notification and access to effective remedy.

33 What do you expect to be achieved by an EU initiative on electronic evidence *?*

	Yes	No	No opinion
* Legal certainty	◉	○	○
* Guarantees for the protection of fundamental rights in accordance with the Charter of Fundamental Rights	◉	○	○

*35 Besides the possibility to set up a legal framework for cases with cross-border dimension, do you think the possible EU initiative should also cover purely domestic cases?

- ○ Yes
- ○ No
- ◉ No opinion

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

58 A possible EU initiative could enable law enforcement authorities to directly request (through a "production request") or compel ("production order") a service provider in another Member State to disclose specific information about a user without having to go through a law enforcement or judicial authority in the other Member State. Do you think a EU initiative should cover

	Yes	No	No opinion
* A direct production request to the service provider (voluntary measure)?	○	◉	○
* A direct production order to the service provider (mandatory measure)?	○	◉	○

59 If the European Commission proposes a legal Framework for direct cross-border requests to service providers: how relevant are the following conditions for a possible cross-border instrument to access e-evidence (Please rate relevance below)?

	very relevant	relevant	somewhat relevant	not relevant	no opinion
* Direct access should only be given for a limited number of offences (e.g. depending on the severity)	◉	○	○	○	○
* Condition that the act is punishable in both countries (double criminality)	◉	○	○	○	○
* Specific safeguards to ensure fundamental rights	◉	○	○	○	○

* Notification of another Member State affected by this measure	◉	○	○	○	○
* Possibility for the notified Member State to object the measure	◉	○	○	○	○
* Notification of the targeted person	◉	○	○	○	○
* Legal remedies for the person affected	◉	○	○	○	○

60 Others : Please specify in the space below

500 character(s) maximum

```
Direct cooperation between law enforcement authorities and service providers
across borders poses serious risks of violation of human rights law (including
data protection). If the Commission were to propose such a framework, in
addition to the safeguards above, we recommend that states publish annual
transparency reports with the number, type, and temporal scope of the data
requests. Companies should also be required to publish transparency reports.
```

61 Data is frequently categorised as non-content (subscriber information, e.g. the name of an e-mail account holder and metadata, e.g. the time an e-mail was sent) or as content (e.g. the content of an e-mail). If the EU would establish a legal framework for the direct cross-border cooperation with service providers, which data should be subject to it?:

	All types of data (content and non-content)	Only non-content data (suscriber information and metadata)
Only data stored in the EU	○	○
Also data stored outside the EU	○	○
Depending on where the service provider is located	○	◉

*62 If the EU would establish a legal framework for the direct cross-border cooperation with service providers, which types of service providers should be subject to it (multiple choice)?

- ☑ Electronic communication service providers (e.g. telecommunications operators, transmission services excluding broadcasting, etc.)
- ☐ Information society service providers (e.g. online services, cloud services, social networks, platforms, etc.)
- ☐ Other digital services providers relevant for investigation measures

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

There could be a situation e.g. during a house search on the suspect's premises where his/her laptop is searched and access to his/her virtualised storage media (cloud-based) is possible directly from the seized device, but it might be unclear where the data is stored or whether there is a cross border dimension at all.

*64 Do you see any need for a common EU framework for this situation?

- (●) Yes
- ( ) No
- ( ) No opinion

65 If the European Commission should decide to propose a legal Framework for this situation, what should the proposal provide?

	Yes	No	No opinion
*Condition that the act is punishable in both countries (double criminality)	●	○	○
*Specific safeguards to ensure fundamental rights	●	○	○
*Notification of another Member State affected by this measure	●	○	○
*Possibility for the notified Member State to object the measure	●	○	○
*Notification of the targeted person	●	○	○
*Legal remedies for the person affected (including challenging the admissibility of evidence)	●	○	○

66 Others : Please specify in the space below

500 character(s) maximum

We would be concerned if direct access to the data were to be effected through hacking of the device. Privacy International questions whether hacking can ever be a legitimate component of state surveillance. Because of its inherent and extensive interference with privacy, as well as the risks that it poses to the security of our devices, hacking for the purposes of surveillance is, prima facie, incompatible with international human rights law.

Part V. International scope

Important service providers are often headquartered in third countries, such as in the US. Alternatively or additionally, the requested data may be stored in a third country. These elements often hamper criminal investigations.

69 In your opinion, what could improve criminal investigations with a third country dimension? (Please rate importance below)

	very important	important	somewhat important	not important	no opinion
*Conclusion of bilateral treaties with main affected third parties	●	○	○	○	○
*Conclusion of multilateral treaties	○	●	○	○	○

* Development of an EU-wide common system/approach	○	◉	○	○	○

70 Others : Please specify in the space below

500 character(s) maximum

States should not carry out evidence-gathering on the territory of another State without the full knowledge and agreement of the targeted State. Improving the efficiency of the MLAT process can be achieved without lowering human rights protection.

Document upload and final comments

72 Should you wish to provide additional information (e.g. a short position paper) or raise specific points not covered by the questionnaire, you can upload your additional document here.

Please note that the uploaded document will be published alongside your response to the questionnaire which is the essential input to this open public consultation. The optional document will serve only as additional background reading to better understand your position.

8a15bff3-16c8-49b4-8cb2-d1aca8718fb4/2017.06.16_UN_Counter-Terrorism_Questionnaire_-_PI.pdf

Contact

EC-E-EVIDENCE-CONSULTATION@ec.europa.eu