Conseil des barreaux européens
Council of Bars and Law Societies of Europe
Association internationale sans but lucratif
Rue Joseph II, 40 /8 – 1000 Bruxelles
T. : +32 (0)2 234 65 10
Email : ccbe@ccbe.eu – www.ccbe.eu

CCBE Response to the Public Consultation on improving cross-border access to electronic evidence in criminal matters

20/10/2017

The Council of Bars and Law Societies of Europe (CCBE) represents the bars and law societies of 45 countries, and through them more than 1 million European lawyers. The CCBE responds regularly on behalf of its members on policy issues which affect European citizens and lawyers.

In this paper the CCBE is responding to the public consultation launched by the Commission on improving cross-border access to electronic evidence in criminal matters. This is an important Consultation and the CCBE wishes to respond to it. However, the questionnaire, which is mainly directed towards public authorities and IT service providers, is structured in such a way as not to elicit responses relating to the area which is a particular concern of the CCBE. Accordingly, it sets out in the present document its response to the questionnaire and makes some further general observations on a possible EU initiative in the area of electronic evidence.

In April 2014, the CCBE published its Comparative Study on Governmental Surveillance of Lawyers' Data in the Cloud. In this paper the CCBE expressed its concerns about the divergence between "normal" rules of search and seizure of evidence and the often much weaker, or even virtually non-existent rules relating to access to digital evidence and interception of data transmissions.

Such regulatory uncertainty becomes particularly hazardous when the data and communications accessed by law enforcement authorities are those that have been granted special protection by the law. This is clearly the case in relation to communications between lawyers and their clients. In all EU Member States, the law protects from disclosure information communicated in confidence between lawyer and client. This principle – usually referred to as 'professional secrecy' or 'legal professional privilege' – has been recognised by most legal jurisdictions for centuries, and was upheld by the European Court of Justice in the AM&S case (C-155/79).

The protection of the secrecy or confidentiality of data in the possession of lawyers subject to such secrecy or confidentiality is a foundation of the rule of law. Regulatory regimes developed independently by all of the jurisdictions across the EU reflect that fundamental norm in their respective rules applying to the conduct of searches and seizure of evidence in lawyers' premises. Whatever the diversity amongst such systems (and there is wide diversity) they all share this value as a common core.

However, the rules have not always kept up with changing technology. Therefore, in some jurisdictions, data in electronic form held in the premises of an IT provider on behalf of a lawyer enjoys less protection than such data stored in the lawyer's own office. The CCBE sees no justification for such a distinction.

If such data is properly regarded by society as requiring protection, then there can be no proper justification for such differentiation. In the modern IT environment, such differentiation is also unnatural: people use the same user interface for access, for sharing, for communicating and for storing data, they do not even recognize when information is sent from one computer to another. It is all the same for the lawyer using the computer whether electronic client data was sent as an email attachment or merely shared with the recipient following the identification of the latter.

A further area of regulatory uncertainty arises due to the circumstance that, in some countries, from the way the relevant lawyers' information protection is worded, it is not clear whether the relevant provisions apply to information stored at outside service providers, like hosting or cloud computing service

providers. Such uncertainties could encourage law enforcement authorities to turn directly to the cloud service provider for information stored in its server or servers (without a court warrant in some countries), instead of going to the lawyer's premises with a proper warrant issued by judicial authority.

These problems are compounded by the circumstance that there is no suitable technical way in which either a hosting or cloud service provider or an outsider (such as a state agency or power) might be able to identify material protected by legal privilege or secrecy.

In view of these ambiguities existing at national level, it is all the more important that any EU initiative regulating cross-border access to digital evidence ensures that sufficient safeguards are in place to protect fundamental rights.

To that effect, the CCBE calls upon the EU institutions to adhere to the following main principles:

A. *The over-riding principle should be that whatever protection is granted in the paper world should also be granted in the electronic world.*

The same principles should be applied to data in a digital context, as is the case with data that is held physically on a person's or an organisation's premises. In the case of lawyers this means that insofar as the rules relating to the physical world of a lawyer's office make special provision for, for example, the attendance of representatives of the lawyer's bar at searches of his office, then an analogous provision should be made for (cross-border) virtual searches. In other words, the use of electronic communications services or other cloud services by lawyers should be protected in the same way regardless of whether the content is stored in a data centre, or in a computer at the lawyer's office or on his person. That may entail further IT standardisation work by the IT service providers, including cloud service providers, but, in CCBE's view this must be done.

B. *Effective regulation should not be reasonably capable of being circumvented. There must be no defaulting back to minimal protection.*

Guarantees should be provided that where there is a strict regime in force to protect lawyers' data, that regime cannot be sidestepped by the relevant authorities making formal or informal cross-border data requests directly to the lawyers' IT service providers to produce the information. When a search warrant is enforced, an organisation should be notified, allowed to assess its legal rights and obligations, and if possible, to be able to challenge the request before any data can be seized. This entails that requests for access to digital evidence should, whenever possible, always be addressed to the data controllers, rather than the data processors.

C. *Whatever regime is established for the cross-border access to digital evidence, that regime should guarantee the inviolability of data and other evidence falling under the principle of legal professional privilege or professional secrecy.*

All the protections established for search and seizure should also apply if the data is to be intercepted cross-border and accessed in transit, as part of a communication, no matter whether the entity technically carrying out the interception is an electronic communications service provider, an IT service provider or an agency of the government acting directly. Content that contains a professional secret or legally privileged information, and that is processed by an electronic communication service or a cloud service provider (including an email service provider), should not be accessible to government agencies.

To that end, law enforcement authorities should be required to use all technological means available to leave material protected by professional secrecy and legal professional privilege out of the scope of surveillance operations. A pragmatic way forward would be to require electronic communications services and cloud service providers to offer lawyers an option for indicating such information – of course, only after careful verification as to whether that user is indeed a lawyer as claimed. For example, in The Netherlands, there exists a telephone number recognition system which is capable of recognising lawyers' telephone numbers and cutting surveillance.

CCBE responses to the questionnaire:

In the list below, only those questions have been copied which are considered to be of relevance to the CCBE. The reply to all other questions not included in the list below is “no opinion”.

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

***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

X 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	X				
*Loss of sovereignty for your Member State					X
* Risk that third countries impose similar obligations to service providers to disclose electronic evidence stored in the EU (reciprocity)	X				

28 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
*Less competences compared to the current situation					X
*Confusing landscape of instruments (EIO, Budapest Convention, MLA)	X				
* Difficulties in enforcing a request		X			

29 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
* Mandatory nature					X
* Increasing volume of requests					X
*Hampering customer's trust in your services	X				

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

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

***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
- X 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)?			X
*A direct production order to the service provider (mandatory measure)?		X	

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)	X				
*Condition that the act is punishable in both countries (double criminality)	X				
*Specific safeguards to ensure fundamental rights	X				
*Notification of another Member State affected by this measure	X				
*Possibility for the notified Member State to object the measure	X				

* Notification of the targeted person	X	○	○	○	○
* Legal remedies for the person affected	X	○	○	○	○

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
- X 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)	X	○	○
* Specific safeguards to ensure fundamental rights	X	○	○
* Notification of another Member State affected by this measure	X	○	○
* Possibility for the notified Member State to object the measure	X	○	○
* Notification of the targeted person	X	○	○
*Legal remedies for the person affected (including challenging the admissibility of evidence)	X	○	○