T-CY Cloud Evidence Group

Criminal justice access to electronic evidence in the cloud - Informal summary of issues and options under consideration by the Cloud Evidence Group[1]

Context

Governments have the obligation to protect society and individuals against crime while respecting rule of law and human rights standards. Securing evidence on computer systems, that is, electronic evidence not only in relation to cybercrime but in relation to any crime, is essential for criminal justice.

The challenges faced by criminal justice authorities have been identified.[2] It is now necessary to focus on specific issues that are to be addressed and move towards options and solutions.

These range from making mutual legal assistance more efficient to direct transborder cooperation with service providers and direct transborder access to data where mutual legal assistance is not feasible; and these must meet data protection and rule of law requirements.

A combination of immediate measures (such as better use of existing instruments, pragmatic solutions based on lessons learnt or online tools) and negotiation of additional international legal solutions should be pursued.

The following issues and options are currently being considered by the Cloud Evidence Working Group of the Cybercrime Convention Committee (T-CY).

Issues to be addressed

Differentiating the data that is required: Subscriber information versus traffic data versus content data

- The type of data most often needed in criminal investigations is "subscriber information". This is followed by traffic data and finally content data. It is therefore crucial to address the issue of obtaining subscriber information.

- Obtaining subscriber information represents a lesser interference with the rights of individuals than obtaining traffic data and in particular content data. However, this is not always reflected in domestic laws on access to evidence. In some States, the requirements for criminal justice access to subscriber information in specific investigations are rather low, while in others court orders may be required. This affects domestic investigations and international cooperation. Further harmonisation of rules for access to subscriber information is needed.[3]

[1] http://www.coe.int/en/web/cybercrime/ceg
[2] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680304b59
[3] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e7ad1

- Subscriber information is normally held by private sector service providers and is typically obtained through production orders.[4] Production orders represent a lesser interference with the rights of individuals and the interests of third parties than the search and seizure of computer systems or the interception of communications.

Mutual legal assistance

- Where electronic evidence is stored in foreign jurisdictions, mutual legal assistance in criminal matters is the primary means to obtain evidence. The MLA process needs to be made more efficient in view of the scale of requests involving electronic evidence and the volatility of such evidence.[5]

Loss of location

- Mutual legal assistance is not always a feasible option. For specific situations, such as where the origin of an attack is unknown, where servers in multiple jurisdictions are involved, or other "loss of location" situations where the principle of territoriality is not applicable, solutions need to be found, including transborder access to data in specific criminal investigations.

- Conditions and safeguards for transborder access to data in specific criminal investigations need to be defined.

- In the absence of international solutions, governments increasingly pursue unilateral solutions. This creates risks to State to State relations and the rights of individuals. A common international solution is required to provide a framework for lawful transborder access to data.

A service provider offering a service on the territory of a State

- Often electronic evidence – be it subscriber information, traffic data or content data – is held by service providers offering different types of services and storing data in different jurisdictions. Clarification is needed as to when a service provider is indeed present or "offering a service in the territory" of a State and is thus subject to a domestic production or other type of coercive order. This would help clarify the applicable law and which jurisdiction has the power to enforce.

- Moreover, if subscriber information can be obtained lawfully through domestic orders, the need for international cooperation and thus the pressure on the mutual legal assistance system would be reduced considerably.

"Voluntary" disclosure by private sector entities to criminal justice authorities in foreign jurisdictions

- Some providers – in particular US-based service providers – may respond directly to lawful requests for subscriber information and traffic data by criminal justice authorities in other jurisdictions where they are offering a service. Service providers may also preserve data upon a preservation request received directly from a foreign criminal justice authority. In such situations, service providers assess themselves whether the request is lawful or whether it serves a legitimate interest and thus whether to preserve data or to disclose

[4] See Article 18 Budapest Convention.
[5] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

traffic data or subscriber information voluntarily. They may also notify their customer of the request, which may compromise a criminal investigation. While the number of direct requests to service providers in foreign jurisdictions is large, provider policies and thus cooperation are volatile and unpredictable. A more stable framework is required.

- The voluntary cooperation model raises concerns regarding data protection and confidentiality requirements so that European providers normally choose not to disclose any data directly to criminal justice authorities in foreign jurisdictions, not even in emergency situations. Solutions need to be identified to ensure that disclosure is in line with data protection and confidentiality requirements.

- In some States the data received directly from providers in foreign jurisdictions is not admissible as evidence in criminal proceedings. This would need to be addressed through reforms of domestic legislation.

Emergency procedures

- In exigent circumstances, swift action to prevent imminent danger to life and public security, that is, emergency procedures would be needed to obtain electronic evidence stored in foreign jurisdictions through mutual legal assistance.

- In exigent circumstances, emergency procedures would also need to be available for obtaining electronic evidence directly from a service provider in a foreign jurisdiction.

Data protection and other safeguards

- Access to personal data under criminal procedure law is a lawful derogation to data protection requirements. The international sharing of personal data between competent public authorities – such as criminal justice authorities – should be in line with data protection requirements if it is based on bi- or multilateral cooperation agreements. The mutual legal assistance process is designed to ensure that rule of law requirements are met and that the rights of individuals are protected, in particular if the data sought are to be used as evidence in criminal proceedings.

- However, MLA is not always feasible. "Asymmetric" sharing of data transborder directly between public and private sector entities is increasing.

- European and international data protection instruments are available covering transborder data transfers either from one private sector entity to another private sector entity or from one competent criminal justice authority to another criminal justice authority. Some instruments allow for asymmetric transborder data transfers from a competent criminal justice authority of one State to a private sector entity in another State in exceptional situations.

- Situations where service providers – or other private sector entities – are prepared to disclose data transborder directly to a criminal justice authority in another State seem not specifically foreseen in current data protection instruments. Providers need to assess themselves whether the condition of lawfulness is met, whether it is in the public interest or whether it is in the legitimate interest of the provider as the data controller. Providers may run the risk of being held liable. A clearer framework for private to public transborder disclosure of data would be required, including conditions and safeguards. This would help service providers avoid situations of conflicting legal obligations.

Options

1. **Legal and practical measures at domestic levels to render mutual legal assistance more efficient**

- This includes implementing the recommendations of the T-CY assessment report on the functioning of the mutual legal assistance provisions of the Budapest Convention adopted in December 2014.[6] The first 15 of these recommendations fall under the responsibility of Parties and do not require new international standards. Recommendations 1 to 15 should, therefore, be implemented without delay.

- Recommendation 8 concerns emergency procedures: "Parties are encouraged to establish emergency procedures for requests related to risks of life and similar exigent circumstances. The T-CY should document practices by Parties and providers." Parties – and the T-CY – should pay particular attention to this recommendation. If necessary, provisions for emergency procedures may need to be made in a Protocol to the Budapest Convention.

- States should facilitate access to subscriber information in domestic legislation by differentiating between traffic data and subscriber information and thus by fully implementing Article 18 Budapest Convention.

2. **Guidance Note on Article 18 Budapest Convention on obtaining of subscriber information and clarification of when a service provider is within the jurisdiction of a criminal justice authority**

- Such a Guidance Note would help States make better use of orders for the production of subscriber information from service providers under Article 18 Budapest Convention. This is a domestic measure and thus does not require mutual legal assistance. Better use of this provision would be an efficient and lawful means to obtain the type of information needed most often in a criminal investigation.

3. **Practical measures to facilitate transborder cooperation between service providers and criminal justice authorities**

- Pending longer-term solutions, practical measures (such as capacity building, sharing of good practices, online resource on provider policies and procedural rules in Parties) could be taken to facilitate more coherent cooperation between service providers and criminal justice authorities, in particular with respect to the disclosure of subscriber information upon a lawful request in a specific criminal investigation but also with respect to emergency situations, and by referring to legitimate interests and applicable data protection requirements.

4. **Protocol to the Budapest Convention**

- Provisions on additional options for more effective mutual legal assistance, including:

[6] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726c

- International production orders (Rec 20 T-CY Assessment Report) or a simplified regime for mutual legal assistance requests for subscriber information
- Direct cooperation between judicial authorities in mutual legal assistance requests (Rec 21 T-CY Assessment Report)
- Joint investigations and joint investigation teams (Rec 23 T-CY Assessment Report)
- Requests in English language (Rec 24 T-CY Assessment Report)
- Audio-/video-hearing of witness and victims
- Emergency procedures (Rec 8 T-CY Assessment Report)

- Provisions allowing for direct transborder cooperation with service providers, such as:

  - Disclosure of personal data by a criminal justice authority to a service provider or other entity in a foreign jurisdiction in specific situations and under specific conditions
  - Legal basis and conditions for disclosure of subscriber information by service providers to criminal justice authorities in foreign jurisdictions
  - Direct preservation requests to providers
  - Domestic legal measures to admit data received from providers in foreign jurisdictions as evidence in domestic proceedings
  - Emergency procedures for direct cooperation with providers in foreign jurisdiction in specific exigent situations

- Clearer framework and stronger safeguards for existing practices of transborder access to data, such as[7]:

  - Transborder access to data with lawfully obtained credentials
  - Transborder access in good faith or in exigent circumstances
  - The power of disposal as connecting legal factor

- Data protection

  - Requirements for transborder transfers of data from a criminal justice authority to a private sector entity in another jurisdiction
  - Requirements for transborder transfers of data from a private sector entity to a criminal justice authority in another jurisdiction.

Note:

These issues and options are currently under discussion. They do not represent the final outcome of the work of the Cloud Evidence Group. The Group will continue its work in 2016, including further meetings with service providers and data protection organisations as well as plenary discussions within the Cybercrime Convention Committee (T-CY), before submitting its conclusions to the T-CY for consideration.

Comments may be sent to:

Alexander Seger, Executive Secretary Cybercrime Convention Committee, Council of Europe, alexander.seger@coe.int

[7] https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e70b6