Conference

Article 15 safeguards and criminal justice access to data

19 – 20 June 2014, Council of Europe (Palais, Room 1), Strasbourg, France

Agenda (draft)

Background

The Budapest Convention on Cybercrime is a criminal justice treaty and – among other things – provides for procedural law powers and international cooperation for specified criminal investigations related to cybercrime and electronic evidence in connection with any crime. Procedural law powers are to be limited by human rights and rule of law safeguards and conditions (Article 15). The Budapest Convention is thus designed to allow State Parties to meet their obligation to protect society and individuals against crime while protecting the rights of individuals when securing electronic evidence for criminal justice purposes.

The evolution and proliferation of information and communication technologies – and with it of crime – are causing major challenges and are adversely affecting the ability of criminal justice authorities to protect people against crime. Challenges include the transnational nature of cybercrime, uncertainty regarding the location of data and jurisdiction, and questions related to transborder access to data for criminal justice purposes.

The Cybercrime Convention Committee (T-CY) – representing the Parties to the Budapest Convention – is undertaking detailed work on the question of transborder access to data and is considering the negotiation of an additional Protocol to the Convention on Cybercrime. In this context it has been engaging for some time in a dialogue with interested stakeholders, including civil society organisations, data protection authorities and industry (such as at Octopus 2012, T-CY Hearing 2013, Octopus 2013).

Issues resulting from this dialogue include in particular the necessity to reconcile the need for law enforcement access to data with human rights and rule of law, including data protection requirements, and to clearly separate the question of access to data within the framework of specific criminal investigations from the issue of surveillance activities for national security purposes.

In December 2013, the T-CY decided to continue the dialogue with interested stakeholders. This Conference – organised under the Project Cybercrime@Octopus – follows up on that decision.
Objective

The conference objective is to identify effective solutions regarding the following:

Criminal justice authorities constantly and increasingly need electronic evidence from other countries for specific investigations. How should they obtain this evidence rapidly and consistent with rule of law and data protection requirements? How should they obtain such evidence in situations where mutual legal assistance procedures are not effective? More efficient international cooperation and adapting rules and procedures for securing volatile electronic evidence in an expedited manner are considered a matter of urgency.

Based on case scenarios, the conference is to focus on:

- the distinction between specific investigations to secure data for specified criminal justice purposes versus surveillance and other activities of national security institutions;
- the challenge of law enforcement access to data in the light of technological developments and crime trends;
- data protection and other human rights and rule of law safeguards;
- possible solutions reconciling the obligation of governments to protect individuals and society against crime with safeguards.

The conference is thus to provide further input to the work of the Cybercrime Convention Committee.

Participation

The conference is open to representatives of civil society organisations, Internet Service Providers (including ISP associations), social media, cloud service providers, e-commerce platforms, members and observers in the Cybercrime Convention Committee (T-CY) and other interested stakeholders.

Participation is subject to registration (see www.coe.int/cybercrime).

Contact

Alexander Seger
Head of Data Protection and Cybercrime Division
Council of Europe
Strasbourg, France
Tel: +33-3-9021-4506
Email: alexander.seger@coe.int

Note: The Cybercrime Convention Committee is also undertaking an assessment of the effectiveness of the mutual legal assistance provisions of the Convention on Cybercrime.
<table>
<thead>
<tr>
<th>Time</th>
<th>Event Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>9h30</td>
<td><strong>Opening</strong>&lt;br&gt;Jan Kleijssen, Director of Information Society and Action against Crime, DG1, Council of Europe</td>
</tr>
<tr>
<td>10h00</td>
<td><strong>Session 1: The Budapest Convention on Cybercrime – state of play</strong>&lt;br&gt;&lt;br&gt;This session is to put the question of law enforcement access to data and applicable safeguards within the context of the work undertaken by the Cybercrime Convention Committee (T-CY).&lt;br&gt;&lt;br&gt;- Overview (Markko Künnapu, Ministry of Justice of Estonia / Alexander Seger, Executive Secretary, Cybercrime Convention Committee)&lt;br&gt;- State of implementation&lt;br&gt;- Assessment of provisions on international cooperation&lt;br&gt;- Guidance Notes&lt;br&gt;- Capacity building&lt;br&gt;- Work on transborder access to data: the rationale&lt;br&gt;- Discussion</td>
</tr>
<tr>
<td>10h45</td>
<td><strong>Coffee break</strong></td>
</tr>
<tr>
<td>11h00</td>
<td><strong>Session 2: Crime trends and technological developments – challenges for law enforcement</strong>&lt;br&gt;&lt;br&gt;This session is to discuss challenges that criminal justice authorities are faced with in the light of the evolution of cybercrime and technological developments.&lt;br&gt;&lt;br&gt;- Cybercrime and electronic evidence: what are the challenges?&lt;br&gt;- Adrian Ionut Bobeica, European Cybercrime Centre EC3, Europol&lt;br&gt;- Inger Marie Sunde, Associate Professor, Faculty of Law, University of Oslo, Norway&lt;br&gt;- Erik Plancken, Ministry of Security and Justice, Netherlands&lt;br&gt;- Branko Stamenkovic, Prosecutor, Serbia&lt;br&gt;- Tour de table</td>
</tr>
<tr>
<td>12h30</td>
<td><strong>Session 3: Criminal justice versus national security</strong>&lt;br&gt;&lt;br&gt;This session is to continue the discussions held the Octopus 2013 conference on the need to separate criminal justice measures related to cybercrime and electronic evidence on the one hand, and national security measures involving the interception and collection of data on the other.&lt;br&gt;&lt;br&gt;- Introductory presentations&lt;br&gt;- Joseph Schwerha, California University of Pennsylvania, USA&lt;br&gt;- Discussion</td>
</tr>
<tr>
<td>13h00</td>
<td><strong>Lunch break</strong></td>
</tr>
</tbody>
</table>
14h30 **Session 4: Criminal justice access to data – Data protection, human rights and rule of law safeguards**

This session is to outline the safeguards that apply with regard to criminal justice access to data.

- Data protection requirements (Jean-Philippe Walter, Chair of the T-PD, Préposé fédéral à la Protection des données et à la transparence, Berne, Switzerland) TBC
- Data protection challenges (Paul Breitbarth, Dutch Data Protection Authority/Manuel García Sánchez, Spanish Data Protection Authority)
- Private sector perspectives (Cornelia Kutterer, Director, EU Relations, Microsoft Europe, Brussels)
- Data Protection and rule of law requirements (Joseph Cannataci, Universities of Malta and Groningen)
- Discussion

16h00 **Coffee break**

16h15 **Session 5: Case scenarios**

In this session practical case scenarios are to be presented. These are to illustrate challenges but also help identify possibly solutions.

- Belgium (Jan Kerkhofs, Prosecutor)
- Portugal (Pedro Verdelho, Prosecutor)
- USA (Betty Shave, Department of Justice)
- Norway (Eirik Tronnes Hansen, Prosecutor, Kripos)
- Singapore (G. Kannan, Deputy Public Prosecutor, Attorney General’s Chamber)
- Discussion

18h00 **End of day 1**

---

**Friday, 20 June 2014**

9h30 **Session 6: Scenarios and possible solutions**

Access to data for criminal justice purposes may involve a multitude of situations and acceptable common solutions that meet rule of law requirements will thus entail complex negotiations. This session is to advance the understanding of issues involved by discussing a number of typical and simplified scenarios.

- Scenarios 1: Transborder access to data stored in another Party with consent
  - Scenario 1a: consent by a physical person
  - Scenario 1b: voluntary disclosure by an ISP or data controller
- Scenario 2: Transborder access to data stored in an unknown location with consent
- Scenario 3: Transborder access to data without consent but with lawfully obtained credentials
- Scenario 4: Transborder access without consent in good faith or in exigent or other circumstances
<table>
<thead>
<tr>
<th>Time</th>
<th>Session Title</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>11h00</td>
<td>Coffee break</td>
<td></td>
</tr>
<tr>
<td>11h15</td>
<td>Scenarios and solutions cont’d</td>
<td>- Scenario 5: Extending a search from one territory to another territory</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Scenario 6: Power of disposal as connecting legal factor in situations where territoriality cannot be determined</td>
</tr>
<tr>
<td>12h45</td>
<td>Session 7: Conclusions</td>
<td>This session is to draw preliminary conclusions as to possible solutions.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- International cooperation</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Transborder access to data</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Other alternatives</td>
</tr>
<tr>
<td>13h30</td>
<td>End of conference</td>
<td></td>
</tr>
</tbody>
</table>