Commission on Crime Prevention and Criminal Justice
Thirty-first session
Vienna, 16–20 May 2022
Item 5 of the provisional agenda
Thematic discussion on strengthening the use of digital evidence in criminal justice and countering cybercrime, including the abuse and exploitation of minors in illegal activities with the use of the Internet

Conference room paper submitted by the Permanent Mission of Canada to the United Nations (Vienna), on behalf of the G7 Roma Lyon Group: Criminal and Legal Affairs Subgroup

The attached conference room paper has been submitted by the Permanent Mission of Canada to the United Nations (Vienna), on behalf of the G7 Roma Lyon Group: Criminal and Legal Affairs Subgroup, for consideration by the Commission under agenda item 5 at its thirty-first session.

* E/CN.15/2022/1.
** This document is reproduced as received by the Secretariat.
Roma Lyon Group: Crime and Legal Affairs Sub-Group

Best Practices on the Handling of Mutual Legal Assistance and Extradition requests involving Child Sexual Exploitation and Abuse Material

Generic Protocol for Handling Sensitive Material

April 2022
Generic Protocol for Handling Sensitive Material

Introduction
On occasion, Central Authorities (CAs) may receive images and other materials that constitute child pornography (CP) by email, mail or fax, including from:

• foreign partners in support of their incoming requests;

• from domestic authorities, as evidence produced in response to incoming foreign requests;

and

• foreign partners in response to an outgoing request.

While it is not an offence for CA staff to possess child pornography in the course of a legitimate criminal law investigation, as it is generally not necessary to review these images to execute an MLAT request, and it is not appropriate for such images to be saved to internal systems, it is preferable that efforts are made to discourage the unnecessary transmission of such images as part of an MLAT request. Tips for preventing any unnecessary receipt and further dissemination of CP by CAs and the steps to take if CAs do receive such material are set out below.

Tips for Preventing Receipt in relation to Incoming Requests

Generally, it is not necessary for images of CP to be included in order to execute an incoming request. A description of the offensive material is usually sufficient.

When providing guidance to a country preparing to send a request to CAs and when seeking additional information on incoming requests involving child sexual exploitation offences, guidance should be made available to remind the requesting country to only send a description of images, and not the images themselves.

Where it is anticipated that CP may be produced as evidence by domestic authorities in response to an incoming request, it is imperative that there be communication about how that evidence will be transmitted to the requesting county at the time that the CA forwards the request to the domestic executing authority. This should include determining whether the evidence should be sent through the CA (on a password protected disk or USB, with the password sent separately), or whether it is possible to transmit the evidence on a police-to-police basis (for example, in cases where materials are printed).

The decision on the appropriate means of transmission may need to be re-visited once the evidence is gathered. The executing authority should be encouraged to consult if they have any questions or concerns regarding transmission at that later stage.
Tips for Preventing Receipt in relation to Outgoing Requests

If CP evidence is expected from a foreign authority in response to an outgoing request, the appropriate transmission should be discussed in the request itself.

Minimizing the risk of further dissemination when the CA receives CP

All team members, including the administrators of the central authority mailbox, are responsible for preventing further dissemination of CP materials to other members of the team.

To minimize the risk of further dissemination, when a new request is received and contains references to child sexual exploitation, the recipient should perform a cursory review of the request and all attachments in order to ensure that it does not contain any CP images before forwarding it to log, to the team leads for review, etc…

Please make sure to report and consult with your team leader and Senior Management Team (SMT) as noted below.

What to do if you receive child pornography

Receipt via email

1. Advise your team leader and SMT of the incident.

2. Gather the following information:
   a. The email(s)
      i. Sender
      ii. Recipient(s)
      iii. Subject line
      iv. Date
   i. Type of the information in the email (general description is sufficient)
   b. Attachments
      i. Name and type (PDF, Word, Excel…)

3. Send the information to both to your CA’s IT and corporate security officials at XXXXXXX and XXXXXXXX. You can attach the email but the document containing the images within the email has to be removed. It is sufficient that one person sends the email for all the recipients.

4. Delete the email(s) from your inbox, deleted items and recover deleted items folders.
5. Ask other recipients to delete the email(s), get the confirmation and update your CA’s IT and security officials.

6. If CP images received from a foreign partner, contact the country in question to advise them that we have deleted the CP images and that we generally do not need the materials to consider their MLA request, that a summary of the material is sufficient. Ask that they modify their request accordingly and re-submit. Ask them not to send the original paper version with the CP. When referring the request to domestic authorities for execution, advise the executing office that the CA has the CP materials on file and determine if they require them for the execution of the request. Transmission is to be discussed.

7. If the CP was received from a domestic competent authority as part of a draft outgoing MLA request, then tell them we have deleted the materials and to re-submit their draft with the necessary modifications (i.e. just describe the CP).

8. Prepare a final report on the incident once it is resolved and send to your SMT.

Receipt by mail

1. Advise your Team leader and SMT of the incident.

2. Put the offending material (printed images, un-protected CD/DVD/USB, etc.) into a sealed envelope and label it with the file name. Indicate on the envelope that the material is confidential and contains offensive material. The sealed envelope can be put in the file pocket until it is determined what should be done with the material (see steps 6-8).

3. DO NOT PHOTOCOPY OR SCAN THE CP MATERIALS. DO NOT PUT IN INTERNAL SYSTEMS.

4. If the materials are accidentally scanned or received via fax, follow the following steps:

   a. Advise your CA’s IT and corporate security officials and provide them with the following information:

      i. The scanner or fax number;
      
      ii. The destination computer number;
      
      iii. Sender (who sent it to the CA, who scanned it);
      
      iv. Recipient(s) (who was the scan sent to);
      
      v. Subject line;
      
      vi. Date;
      
      vii. Type of the information in the document (general description is sufficient)
5. Send the information to both your CA’s IT and corporate security officials at XXXXXXX and XXXXXXXXX. Do not forward the scan/images.

6. If received from a foreign partner, contact the country in question and:

   a. Advise them that we do not need the materials to consider their MLA request, that a summary of the material is sufficient.

   b. Ask if any of the documents/disks in the package are originals which cannot be replaced (if this is the case, there is the possibility that the police can return the materials to the country of origin, including via any police liaison officers).

7. If the materials were part of an incoming request, when referring the request to domestic authorities for execution, advise the executing office that the CA has the CP materials on file and determine if they require them for the execution of the request. Transmission is to be discussed.

8. If the material is evidence that should be provided to foreign authorities, the relevant coordinating unit of the national police force which deals with child exploitation investigations, should be approached to see if they can assist with arranging for its transmission (ex. printed material, unsecured CD/USB).

9. Consult with your team leader regarding the final disposition of the material and/if there is any uncertainty on how to proceed.

10. Prepare a final report on the incident once it is resolved and send to your SMT.