

LEGAL CHALLENGES FOR LAW ENFORCEMENT COOPERATION IN CHILD PORNOGRAPHY CASES - THE ROLE OF LEGISLATION -

Workshop of the PNI Institutes

11.04.2011, UN Crime Commission

Prof. Dr. Marco Gercke, Director Cybercrime Research Institute

CHALLENGES RELATED TO ONLINE CP

WHAT WE KNOW

- In the past child pornography was traded offline
- The production in general required the involvement of service provider (film laboratories)
- Similar situation with regard to the distribution that required the involvement of a limited number of service providers (postal services)



Picture removed in print version
Bild zur Druckoptimierung entfernt



Film Laboratory

WHAT WE KNOW

- Availability of Video Cameras changed the situation dramatically.
- With a video camera the offender did not need to rely on service provider to produce child pornography
- Decreased the possibility to identify the offender within the production / duplication process
- Limited means of distribution remain a strong possibility for investigation



Picture removed in print version
Bild zur Druckoptimierung entfernt



Video Camera

WHAT WE KNOW

- Today child pornography is available online
- Global phenomenon
- Influences the way how child pornography is distributed. Today it is possible to host files anywhere in the world and make it available for any user
- Means of distribution are classic services like WWW and email but also less popular services like filesharing



Picture removed in print version
Bild zur Druckoptimierung entfernt



SOURCE: Steel, Child Ab & Neg. 09, 563

SPEED OF DATA TRANSFER

- Data transfer speed enables quick move of data
- Offenders can make use of the speed of data transfer processes to hinder the removal of information



Picture removed in print version
Bild zur Druckoptimierung entfernt



MOVEMENT WEBSITE

MISSING SCIENTIFICALLY RELIABLE DATA

WHAT WE KNOW

- Many figures and numbers that are frequently quoted in the context of discussions about online child pornography are inconsistent
- There is still a lack of scientifically reliable data
- The following examples try to underline the dimension of the problem

SEARCH ENGINES


- Source: Organized Crime Situation Report 2005, Council of Europe, page 36
- It is widely accepted that offenders use the Internet to distribute and get access to child pornography
- However, the search for the term “child pornography” does not mean that the person is searching for images – it could also be a search for legislation

100.000 search engine requests for child pornography daily

 Council of Europe

SEARCH ENGINES

- It is known that offenders can use search engines in their attempt to identify websites
- Most search engine providers have undertaken measures to prevent the use of their services to identify such websites („blacklists“)
- But such technical solutions should not hinder the access to material related to the political and legal debate about the topic


 Picture removed in print version
Bild zur Druckoptimierung entfernt

 Google

TECHNOLOGY USED

- Source: Wolak/ Finkelhor/ Mitchell, *Child-Pornography Possessors Arrested in Internet-Related Crimes: Findings From the National Juvenile Online Victimization Study*, 2005, page 9
- There are several technical tools available that enable offenders to further increase the difficulties in investigating such cases

17% used password protection, 3% evidence-eliminating software (3%) and only 2% used remote storage systems

 Symantec

LEGAL CONSEQUENCES

INTERNATIONAL COOPERATION

- National sovereignty is one of the most fundamental principles of international law
- An investigation of transnational Cybercrime therefore requires the cooperation of law enforcement agencies of all countries involved
- In many instances international cooperation requires dual-criminality



Picture removed in print version
Bild zur Druckoptimierung entfernt



NATIONAL SOVEREIGNTY

INTERNATIONAL COOPERATION

- Various approaches to restrict the principle of national sovereignty in order to speed up investigations failed
- One example for such approach is Art. 32b of the Convention on Cybercrime



Convention on Cybercrime

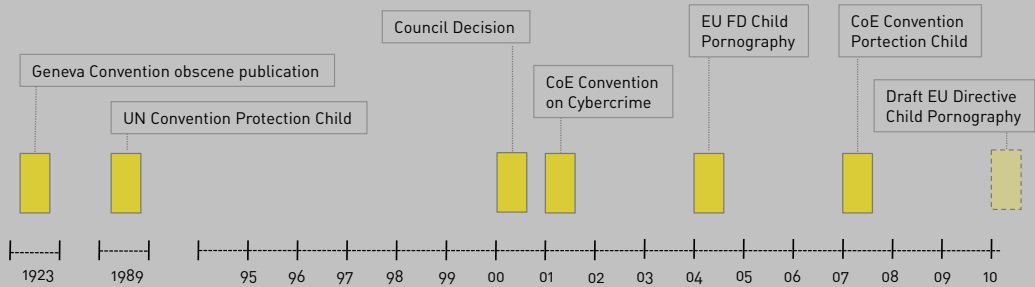
Article 32 – Trans-border access

A Party may, without the authorisation of another Party:

[...]

b) access or receive, through a computer system in its territory, stored computer data located in another Party, if the Party obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to the Party through that computer system.

LEGISLATION / POLICY COE/EU/UN



EXTENT

- Harmonisation approaches focus on basic aspects and often leave space for reservations – details of criminalization can vary significantly
- Example: Art. 9 Convention on Cybercrime
- The fact that two countries ratified an instrument does not necessary mean that they criminalize to the same extent

Convention on Cybercrime

Article 9 – Child Pornography [...]

(3) For the purpose of paragraph 2 above, the term “minor” shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

(4) Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

GAPS

- As cooperation requires legislation gaps can have significant impact
- In the early discussion about legal response to an online distribution of child pornography the drafter of regulations focused on digital images
- Today not only images and videos but also audio recordings of the sexual abuse of children are distributed online
- Older approaches often use language (such as “visually” or “image”) that excludes such material

Convention on Cybercrime

2. For the purpose of paragraph 1 above, the term “child pornography” shall include pornographic material that visually depicts:

- a. a minor engaged in sexually explicit conduct;
- b. a person appearing to be a minor engaged in sexually explicit conduct;
- c. realistic images representing a minor engaged in sexually explicit conduct.

GAPS

- Countries are still struggling with the implementation of legislation related to online child pornography
- Example: Germany
- Reference to “written materials” leads to difficulties in the application of the provision to online child pornography

German Penal Code

Section 184b - Distribution, acquisition and possession of child pornography
(1) Whosoever
1. disseminates;
[...]
pornographic written materials (section 11 (3)) related to sexual activities performed by, on or in the presence of children (section 176 (1)) (child pornography) shall be liable to imprisonment from three months to five years.

German Penal Code

Section 11 - Definitions
[...]
(3) Audiovisual media, data storage media, illustrations and other depictions shall be equivalent to written material in the provisions which refer to this subsection.

GAPS

- Various 24/7 networks that can be used to speed up international cooperation
- However, two studies, that analysed international cooperation based on the Council of Europe Convention on Cybercrime came to the conclusion that not even all countries that ratified the Convention established such contact point.
- Another finding was that those countries that did establish a contact point often enough only use it for very limited purposes

CoE Convention on Cybercrime

Art. 35 – 24/7 Network

Each Party shall designate a point of contact available on a twenty-four hour, seven-day-a-week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

- a) the provision of technical advice;
- b) the preservation of data pursuant to Articles 29 and 30;
- c) the collection of evidence, the provision of legal information, and locating of suspects.



Cybercrime Research Institute
Prof. Dr. Marco Gercke

Niehler Str. 35
D-50733 Cologne, Germany
gercke@cybercrime.de
www.cybercrime-institute.com