1. ------IND- 2009 0371 D- EN- ------ 20090720 --- --- PROJET

Preface

Draft act on combating child pornography in communications networks

of …2009

A. Problem and goal

In spite of national and international efforts to identify offenders and shut down web sites, child pornography sites offering content are still available on the Internet and are steadily on the increase. .The goal of the draft act is to make access to this type of content more difficult.

B. Solution

Adoption of a legal obligation, for service providers that provide access to communications networks (access mediators), for the implementation of technical measures to hinder access to child pornography on the Internet.

C. Alternatives

None.

D. Financial impact on public budgets

1. Budgetary expenditure excluding implementation costs

None.

2. Implementation costs

Additional expenditure, which will be incurred in the context of the single plan 06, will be borne by the Criminal Investigation Department with regard to the creation and updating of a list of child pornography content as well as with regard to the provision of a blacklist.

E. Miscellaneous costs

Service providers will incur investment costs for the technical provisions which are intended to make access to child pornography on the Internet more difficult. There will, in addition, be

expenses for the current business and for the setting up of a stop message. These costs are generally not quantifiable and depend, among other things, on which technical approach is chosen to hinder access, the respective business model, the network structure and the number of customers the service provider has. For economic reasons, an estimate of the actual accumulated costs is not possible at the moment. Indirect costs for companies and households incurred by unintended restrictions to Internet use and effects on flat rates, e.g. for services provided, cannot be excluded. Effects on general price levels, in particular on the consumer price level, are not to be expected, however.

F. Bureaucracy costs

The draft act contains a new information obligation for businesses. It concerns the transmission by the service provider of a list of attempts to access child pornography sites (Sec. 8 a par.6 TMG - German Broadcast Media Act). It is to be assumed that the drawing up and transmission of this information will, as far as possible, be done automatically and will not incur any appreciable costs for the company concerned.

Draft act on combating child pornography in communications networks

of …2009

The Bundestag has decreed the following act:

Article 1

Amendment to the German Broadcast Media Act

The German Broadcast Media Act of 26 February 2007 (Federal Law Gazette - BGBl. I p. 179), as amended by Articles 2 of the Act of 25 December 2008 (BGBl. I p. 3083), is amended as follows:

1. The following Sec. 8a is inserted after Sec. 8:

"Sec. 8a

Hindering access to child pornography in communications networks

(1) Within the context of its task as central office pursuant to Sec. 2 of the (German) Federal Criminal Investigation Department Act, the Federal Criminal Investigation Department generates a list of fully qualified domain names, IP addresses and destination addresses of broadcast media providers who, pursuant to Sec. 184b of the penal code, contain child pornography, or whose purpose is to point to child pornography sites on such broadcasting media (blacklist). Within the meaning of paragraph 2, service providers must be informed when the blacklist - updated on work days - becomes available.

(2) Pursuant to Sec. 8, service providers who provide access to information via a communications network to at least 10,000 users or other authorised users against payment, must implement appropriate and reasonable technical measures to hinder access to broadcasting media that appear on the blacklist. Fully qualified domain names, IP addresses and destination addresses of broadcasting media may be used to block access. The blocking occurs at least on the level of the fully qualified domain names which are not blocked in the associated IP addresses. The service providers must implement the measures immediately, or at the latest within six hours after the Criminal Investigation Department has made available the current blacklist.

(3) The service providers must secure the blacklist information by suitable means against third parties who are not involved in implementing of the blocking.

(4) The service provider reroutes user inquiries (stop messages) which are consulted on broadcasting media and which appear on the blacklist to one of the broadcast media providers operated by them in order to inform the user of the grounds of the blocking and provide the option to contact the Federal Criminal Investigation Department. The Criminal Investigation Department makes the arrangements.

(5) Service providers may, as far as it is necessary for carrying out the measures pursuant to paragraphs 2 and 4, collect and use personal data. This data may be transmitted to the competent authorities at their request for the purpose of pursuing crimes, pursuant to Sec. 184b of the penal code.

(6) The service providers transmit weekly an anonymous list to the Criminal Investigation Department detailing the number of attempted accesses per hour to the broadcasting media on the blacklist.

(7) The service providers only answer when and in as far as they do not implement the blacklist with measures according to paragraphs 2 to 6.

(8) The Criminal Investigation Department is obliged to make documents readily available for which it can be proved that the entries on the blacklist meet the preconditions pursuant to paragraph 1 at the moment of their rating by the Criminal Investigation Department. It passes on information to service providers in the meaning of this law who, on request, state a justified interest in whether and in which period a broadcasting media is or was included on the blacklist.

(9) In which form and according to which procedure the blacklist and drawing up pursuant to paragraph 6 are made available, is regulated by the Criminal Investigation Department with the cooperation of the service provider by means of a technical directive.

(10) The basic right of telecommunications secrecy (Article 10 of the Basic Constitutional Law) is restricted to paragraphs 2, 4 and 5.This concerns telecommunications activities in the meaning of Sec. 88, paragraph 3, point 3 of the Telecommunications Act."

2. In Sec. 16 paragraph 2, the following numbers 1a and 1b are inserted after number 1:

"1a) contrary to Sec. 8a paragraph 2 sentence 1 or 4 a measures not taken or not taken on

time,

1 b) contrary to Sec. 8a paragraph 3, the blacklist is not secured, not properly secured, or not completely secured",

Article 2

Amendment of the Telecommunications Act

The Telecommunications Act of 22 June 2004 (BGBl.I p. 1190), as amended by Article 16 of the Act of 17 March 2009 (BGBl.I p. 550), is amended as follows:

1. In Sec. 96 paragraph 1, the part preceding number 1 is worded as follows:

   "The service provider may only collect the following traffic data and only for purposes as described in this section or in Sec. 8a paragraph 2 or paragraph4 of the Telecommunications Act, and use the data not later than until the end of the connection":

2. Sec. 149 paragraph 1 number 16 is worded as follows:

   "16. use data contrary to Sec. of 95 paragraph 2 or Sec 96 paragraph1 or paragraph2 sentence 1 or paragraph3 sentence 1"

Article 3

Evaluation

The Federal Government makes a report to the Bundestag within two years after entry into force concerning the application of this act.

Article 4

Entry into force

The act enters into force on the day following its promulgation.