



Telecommunication Industries Association in Denmark

IT section

Copenhagen (Denmark), January 17th 2007

Guidelines for the handling of requests regarding criminal activity on the Internet

Background

In February 2005, the ISP members of the Danish IT Industry Association (ITB) and Telecommunications Industries Association (TI) agreed to carry out a study designed to identify opportunities for ISPs to use self-regulation to combat, in a more focused way, undesired behaviour and criminal activity on the Internet. The initials "ISP" stand for "Internet Service Provider".

The Danish National IT and Telecom Agency (ITTST) then turned to the ITB and TI to obtain details of action taken by ISPs against undesired behaviour and criminal activity on the Internet. The knowledge so gained went on to form part of an ITTST ["ITST" in the original] report submitted to the Danish minister of science and technology.

It was against this background that the ISP members of the ITB drew up this code of conduct designed to control undesired behaviour and criminal activity on the Internet. They also agree that the code should be subject to an annual review and revised as required.

Scope

The obligations of ISPs regarding the transmission and storage of data over the Internet are now primarily subject to the rules contained in articles 15 and 16 of the Danish law governing e-commerce (*e-handelsloven*). This regulatory framework establishes that providers of services covered by this law are not obliged to take their own steps to monitor the content of the information that ISP customers store using the service provider's facilities. Internet service providers do however run a risk of being held liable for not responding to enquiries concerning harmful content.

It is likewise apparent that the rules on liability contained in Danish legislation covering media responsibility do not apply to the type of Internet services covered here. It would also be difficult, under the terms of Danish e-commerce legislation, to envisage any liability under criminal law; partly because Danish law follows the principle of *lex specialis*, and also because wilful intent (*mens rea*) would only rarely be involved.

Action regarding undesired online behaviour can be initiated either by direct notification or on the basis of evidence found by ISP staff.

The ISPs concerned have now agreed to classify undesired conduct into two main categories:

1) Undesired behaviour of a technical nature (hacking, spam, virus propagation, etc.)

and

2) Criminal acts committed via the Internet, given the specific opportunities offered by the web to conceal illegal activity with relative ease.

Actions covered by point 1 are regulated by a separate sector-specific code of conduct, and will therefore not be discussed any further here.

This code of conduct is therefore concerned only with infringements that are covered by point 2, and where it is agreed that relevant criminal offences are involved, including:

- child pornography
- indecent exposure
- racist remarks
- threatening behaviour

Procedures

The above obligations under Danish e-commerce law, along with requests from authorities, organisations representing special interests and users, are dealt with by various means.

Internet service providers that are already regulated by the ISP security forum, for instance, are subject to a separate code of practice on child-pornography filtering, designed to combat the spread of this type of material.

Examples of typical procedures regarding cases of criminal activity on the Internet

1. Whenever criminal offences relating to racist remarks, threats and/or indecent exposure are reported, they are initially handled by the ISP's postmaster using the following procedures:
 - The complaint is registered, and the person reporting the incident is urged to contact the local police.
 - If the consequences of the incident reported are such that direct evidence is clearly required, or that it is relevant given the nature of the complaint, an employee responsible for postmaster-related issues must immediately secure this evidence, provided it is legal to do so.
2. Criminal offences relating to the possession and distribution of child pornography are subject, in such cases, to the following procedures:
 - The ISP's postmaster receives and records the complaint.
 - A check is made to verify if the material constitutes child pornography.
 - If there is no doubt that the material contains child pornography, the matter is immediately reported to the police. If the police so request, the evidence and material are sent to the police along with any other relevant, legally-obtained information. The ISP will then, subject to the corresponding police request, block access to the website or newsgroup where the material was found.
 - If there is **any** doubt as to whether the material constitutes child pornography (e.g. due to difficulties determining the age of the persons depicted), the matter is left in the hands of the police, who will carry out the corresponding assessment.
 - If the police consider that a criminal offence has been committed, they may ask for details of the customer's geographic location, so as to be able to assign the case to the corresponding local police force. The ISP will then disclose this information.

- Court orders and other rules may stipulate that further relevant material be disclosed to the police in connection with the investigation of the case.
- The ISP considers whether to issue a response with respect to the user (see subscription terms and conditions).
- If there is a specific evaluation to the effect, access to newsgroups may be blocked in cases where there are posed images that are not covered by article 235 of the Danish Penal Code, but where there is no doubt regarding the purpose of the pictures concerned, provided the police – after considering the matter – ask the ISP to do so.

This code of conduct is applicable from January 22nd 2007 onwards.

With best regards,

pp M. Tolstrup
Managing Director

Henrik Egede
Deputy Managing Director

TI – Telecommunication Industries Association in Denmark

IT section