

**Study Group on Countermeasures against Illegal/Harmful Information
on the Internet—7th Meeting
Summary of Minutes**

1. Date and Time

Thursday, July 17, 2008; 14:30–16:30

2. Location

Hall, 2nd basement, MIC

3. Attendees (honorifics omitted)

(1) Sub-Council Members

Keigo Inoue, Hisamichi Okamura, Takamasa Kishihara, Tamayo Kimura, Masanori Kusunoki, Tetsuo Yagami (proxy for Kuwako), Fumiaki Koizumi, Akio Kokubu, Masanori Koshiyama, Makoto Saito, Satoshi Seki, Taiyo Takahashi, Nobuyuki Takahashi, Tsuyoshi Takenouchi, Toshiaki Tateishi, Hiroshi Tano, Miki Nagata, Makoto Haruta, Naoya Bessho, Masao Horibe, Toru Maruhashi, Seiji Yoshikawa, Masahiro Wakai

* Kato, Sakata, Takahashi, Hasebe, Hirasawa, Matsuyama and Yamaguchi were absent.

(2) Observers

Counselor (IT Office), Cabinet Secretariat; Director for Policy of Youth Affairs, Cabinet Office; Cybercrime Division, National Police Agency; Youth Division, Ministry of Education, Culture, Sports, Science and Technology

(3) MIC Representatives

Sakurai (Director-General, Telecommunications Bureau), Takeuchi (Director-General, Telecommunications Business Department), Ando (Director, General Affairs Division, Telecommunications Bureau), Nagashio (Director, Computer Communications Division), Katagiri (Senior Planning Officer, Telecommunication System Division), Ninomiya (Director, Telecommunications Consumer Policy Division), Omura (Senior Planning Officer, Telecommunications Consumer Policy Division), Okamura (Assistant Director, Telecommunications Consumer Policy Division), Ouchi (Assistant Director, Telecommunications Consumer Policy Division), Murohashi (Assistant Director, Telecommunications Consumer Policy Division)

4. Agenda

(1) Opening address

(2) Subjects

(i) Summary of the Act on Secure and Safe Internet Use Environment for the Youth (Secretariat)

(ii) Status in other countries on countermeasures against illegal/harmful information

Tomoki Takahashi, Chief Researcher, Mitsubishi Research Institute, Inc.

(iii) Planning of the Safe Network Development promotion program (Secretariat)

(iv) Future Schedule (Secretariat)

(3) Closing

5. Meeting Summary

(1) Opening address

(2) Subjects

(i) Summary of the Act on Secure and Safe Internet Use Environment for the Youth (Secretariat)

The secretariat gave a presentation based on References 3-1 and 3-2.

(ii) Status in other countries on countermeasures against illegal/harmful information

Mitsubishi Research Institute, Inc. Chief Researcher Takahashi gave a presentation based on Reference 4. The following questions and answers were subsequently asked and given.

Q: In the description, "making it obligatory for the carriers to provide filtering tools for children and youth for free," on page 8, "providing tools" seems to be regular software distribution, like the distribution of filtering software that is widely carried out in France.

Alternately, does this simply mean providing a filtering service?

A: It means making it obligatory to provide a filtering service.

Q: On "if an ISP finds that child pornography content has been uploaded to a server under its control, it must call the Cyber Tipline set up in the NCMEC" on page 1, what will happen if the ISP does not notify the NCMEC? What does "cuts off" mean in "the provider/hosting company cuts off access" in the last paragraph on page 8? Does it indicate deleting the information? On "provide a system for verifying age" on page 9, does it mean asking for submittal of identification, as in Korea? In addition, on "a removal order to providers" in the table on page 11, what is the scope of "providers?" Does it include content providers?

A: In the United States, it has been made obligatory for an ISP to notify the NCMEC if it finds that child pornography content has been uploaded. If an ISP is not aware of it, the ISP must do nothing. We have no knowledge about what will happen if the ISP fails to notify the NCMEC. I think "cut off access" on page 8 is implemented through filtering. We do not know the details of such as deletion of information. The "system for verifying age" on page 9 is a procedure performed when making a contract. The service provider receives credit card information and other information for certification of a user and it starts providing services after it has confirmed the validity of the information. On page 11, we used the term "providers" to summarize items in a table. They are referred to in various ways, such as content providers, in each country.

Q: I also conducted a survey on other countries. The obligation of notification in the United States is stipulated by law. If an ISP knows that child pornography content has been uploaded and fails to notify the NCMEC, the ISP is fined, and if the ISP fails a subsequent time, the amount of the fine is raised. As opposed to Japan, mobile phones with Internet access are not widespread in other countries. From what I heard from a local carrier association, no problem has occurred officially. What are the realities on this issue?

A: A hearing that we conducted also indicates that they have experienced no such problem.

Q: On the descriptions of access restriction services in other countries such as "service for prohibiting youth from accessing adult sites" (on page 1), "categories defined by the IMCB" (on page 4), and "the IWF blacklist" (on page 4), we would appreciate you explaining later on, for each case, who restricts access to problem sites and in what framework these restrictions are discussed.

A: We have investigated the categorization of content and will provide a summary of the investigation to you later.

Q: The Reference says that in Australia and Korea, the office of jurisdiction is authorized to order providers to delete content. Are the targets of deletion limited to illegal information or do they include harmful information?

A: I suppose the targets in principle are illegal information. For a detailed distinction, I will examine this later.

Q: On limitation of liability, is the limited liability restricted to that which occurs due to copyright infringement, or does it mean an entire civil case liability? Does it also include criminal liability? We would appreciate you investigating the scope of liability.

(iii) Planning of the Safe Network Development promotion program

The secretariat gave a presentation based on References 5-1 and 5-2. The following questions and answers were subsequently asked and given.

Q: Outbound Port 25 Blocking (OP25B), a countermeasure against spam, is widespread in Japan and it has yielded quite practical results. When I talked about this topic in other countries, many people did not even know how to implement OP25B. I think it is important to introduce such efforts in Japan to overseas. The program seems to describe only disadvantages and their countermeasures for the Internet. We would like you to also mention good points.

Q: On "promote, in principle, making mobile phone filtering for users younger than 18 obligatory " in 1 (1) of Reference 5-1, I think the filtering obligation has been implemented by the Act on Secure and Safe Internet Use Environment for the Youth, which was concluded in June, unless this is concerning the discussion on the enforcement of the law. If so, I think that many parts should be dealt with by the discussion on voluntary efforts.

A: You are right. Mobile phone filtering has been made obligatory by law, and the law should be properly enforced. We need to discuss the enforcement. If any problem were found, it would be necessary to establish a system for solving it.

Q: I personally think it is not necessary to limit the liability of providers on illegal information. In any case, this topic requires detailed discussion. For voluntary efforts, we would like you to support the civil efforts such as the Content Evaluation and Monitoring Association (EMA) and the consultation for operators.

A: At this point in time, we do not intend to compile specific results. We would like you to discuss that issue, including whether or not to reform laws.

Q: The laws concerning this program should include those within the jurisdiction of other ministries and agencies. We would like you to announce the program as total measures that include the laws and regulations of each ministry and agency. For example, when the Act on Specified Commercial Transactions was amended at the same time as the Act on Regulation of Transaction of Specified Electronic Mail, for the users and operators, both laws overlapped for the most part, but there was a slight discrepancy in obligation. Inconsistency among related laws and regulations can cause confusion to the users and operators. We hope careful discussions will be conducted on this matter.

A: We will discuss paying attention to the point you specified.

Q: For the Act on Secure and Safe Internet Use Environment for the Youth, I have heard that there were much more severe proposals, but through the discussions on the boundaries

within which the government should engage itself, the current provisions were settled. Without proper understanding of such details, there are possibilities that considerably severe controls may be established at local government levels. Therefore, it is necessary for the central government to explain in detail why strict legislative controls were not implemented, the story behind that and the philosophy to the local governments so that relevant information is shared. When inventing various measures, it is natural that we find merits and demerits. When the local governments review the measures, it is preferable that proper administrative evaluations be made on the merits and demerits, and that the measures are implemented in each area effectively and with little harmful effect.

A: Municipalities often asks us about the issues on the Internet. As the law has now been enacted, we will be able to respond to those questions based on a firm foundation. Through such back-office negotiations, we intend to work on making municipal ordinances more moderate and replacing them with campaign activities.

Q: For regulations by municipalities, needless to say, the issues of ordinances more strict than the laws they are based on and the handling of municipal libraries is a controversial topic. For those within the jurisdiction of the pertinent local governments, some ordinances are more stringent than the corresponding laws. There is also a lack of unity among local governments, which should be eliminated to some extent.

Q: The Act on Secure and Safe Internet Use Environment for the Youth stipulates that the Committee for Promoting Countermeasures against Harmful Information on the Internet and Improvement of Internet Use Environment for the Youth established in the Cabinet Office should lay down a general plan. What is the relationship between the general plan and the Safe Network Development promotion program?

A: The general plan will be laid down after the law comes into effect, which is within a year from promulgation. Therefore, discussions will not start immediately. However, the problems on the Internet we are facing require prompt countermeasures. Considering this, we are planning for MIC to formulate a basic philosophy and, if possible, some of it will be reflected in the general plan. The general plan only targets information harmful to youth according to the laws it is based upon. Illegal information and information harmful to everyone will possibly not be targets of the general plan and will be discussed among our staff.

(iv) Future Schedule

The secretariat gave a presentation based on Reference 6. The following questions and

answers were subsequently asked and given.

Q: From the experience of working in the Internet Hotline Center, most requests to delete illegal information are accepted possibly because of the fear of liability that occurs if the information is left undeleted. On the other hand, for harmful information, some operators operate on original policies that are devoid of common sense. Those operators seldom accept deletion requests. We would like the Basic Framework Working Group to discuss how to deal with such operators who intentionally do nothing.

A: We understand the existence of the problem. The purpose of the Voluntary Efforts Working Group is to make a distinction between the operators who properly take measures and those do not. It is also required to discuss what measures can be taken against problem operators. We will keep ourselves flexible in which Working Group discusses what subjects. The first meeting of each Working Group will discuss these topics and make their agenda more clearly.

Q: Why are Working Group discussions not open? Many of the Basic Framework Working Group members are access providers, but as they also discuss content, content providers should also participate.

A: The reason for closed discussions is to promote frank exchange of opinions among the various parties concerned, but the items that will be reflected in the program will be released through this meeting. For the members of Basic Framework Working Group, the discussion on the limitation of liability is specified by a supplementary provision of the Act on Secure and Safe Internet Use Environment for the Youth, and we thought it was appropriate to gather the members who discussed the Act on the Limitation of Liability for Damages of Specified Telecommunications Service Providers and the Right to Demand Disclosure of Identification Information of the Senders. The members are not fixed. They may be reshuffled according to the progress of the discussion and in consultation with the Chief.

Q: How much of the minutes and meeting summary of the Working Group discussions are released? How much information is supplied to the advisers?

A: We do not intend to make the Working Group discussion too formal, but the content of discussion will be reported in detail to the advisers. We would like the advisers to give various opinions on the discussions, who should be interviewed, and the operation of the Working Groups.

- The next meeting is scheduled for mid-September.

(3) Closing