Summary of Minutes of the 18th Meeting of the Round Table Conference on the Privacy of Information in the Telecommunications Service Sector

1 Date and time: January 23 (Mon) 2006 13:30 to 14:50

2 Location: Conference Room 801 (8F), Ministry of Internal Affairs and Communications

3 Attendees:

(1) Members:	Kuwako, Kohai, Saeki, Tagaya (Acting Chairman), Tajima, Nakamura, Hirukawa, Fukumoto, Bessho, Horibe (Chairman), Murakami
(2) Ministry of Internal Affairs and Communications:	Suda (Director-General of the Telecommunications Bureau), Terasaki (Director-General of the Telecommunications Business Department), Furuichi (Director of the Telecommunications Consumer Policy Division), Yajima (Senior Planning Officer), Shibuya (Assistant Director), Ikeda (Assistant Director)

4 Outline of proceedings

(1) Opening

(2) Filtering and the confidentiality of communications

(3) Exchange of subscriber information in cases of spam mail transmission (report)

(4) Closing

5 Major discussions

- Separately attached: The details regarding the relationship between the filtering of e-mails conducted by telecommunications service providers and Article 4 (Protection of the confidentiality of communications) of the Telecommunications Business Law, were examined and the basic concept

of the relationship was agreed on.
(Major discussions were as given below.)

- It will be necessary to discuss hereafter the application standard which will be used as a guide for providing actual services, as they apply to each condition for telecommunications service providers when providing a filtering service for spam mails and the like (hereinafter “Service”), once the initial setting has been made effective.
- In addition to conditions relating to the provision of the Service by telecommunications service providers after making the initial setting effective, it is also necessary to discuss: the obtaining of effective consent from existing users who use the Internet under the contract; the handling of cases where the content of the Service once agreed upon is to be changed; and the building of a system to address the explanations and inquiries regarding “over block.”
- The details regarding the setting of the Service provided by telecommunications service providers are important factors for determining whether or not we can say effective consent has been given. Thus the details should be fully explained to users and at the same time made reasonable for general users.
- Regarding the Service provided by telecommunications service providers, the settings are only made effective after users complete their subscriptions. Therefore, users who do not know the existence of the Service tend to have no opportunity to subscribe to the Service. The provision of the Service by telecommunications service providers upon making the initial setting effective may be useful in that it could act as a catalyst in helping to introduce the Service a to users who are unfamiliar with it.

(End)

Relationship between the e-mail filtering conducted by telecommunications service providers and Article 4 (Protection of the confidentiality of communications) of the Telecommunications Business Law

No.1 Background

1. In recent years, e-mail filtering has been used and proved effective as a measure against advertising mails (spam mails) that are sent unilaterally without obtaining the consent of the recipient. Generally speaking, e-mail filtering means mechanically searching the content of a particular e-mail and detecting and then blocking the e-mail if its content corresponds to a given preset condition. One concrete example is that of key word filtering in the text of e-mails (searching if a preset keyword is included in the text of the received e-mail and blocking the e-mail if it includes the keyword).
   Filtering is mainly divided into two categories: cases where users purchase or download commercial filtering software from the Internet to install in their terminals; and cases where telecommunications service providers (hereinafter “Providers”) conduct filtering on the servers controlled by them.
   When e-mail filtering is conducted on the servers controlled by Providers, it will promote the prevention of spam mails if it is properly done, but it may damage the interests of users in terms of the confidentiality of communications stipulated in Article 4 of the Telecommunications Business Law (hereinafter “Business Law”) of users if it is used illegally.
   Accordingly, we will make the e-mail filtering conducted by Providers consistent with the protection of the confidentiality of communications stipulated in Article 4 of the Business Law.
2. As mentioned above, e-mail filtering is mainly divided into two categories; cases where users install filtering software in their own terminals; and cases where filtering is conducted on servers under the control of Providers.
   Regarding the relationship between the e-mail filtering and the protection of the confidentiality of communications stipulated in Article 4 of the Business Law, what we need to consider are cases where e-mail filtering is conducted on servers under the control of Providers, since Article 4 stipulates that, “the confidentiality of communications which telecommunications service providers become involved with

during handling must not be violated".
Consequently, e-mail filtering will hereafter mean: "Providers, with a particular purpose, mechanically searching for matters that come under the category of the confidentiality of communications regarding e-mails that they become involved with through handling, and detecting and blocking those that match the given preset condition."

No.2 Deliberations

1. Items that fall under the category of the confidentiality of communications
   The confidentiality of communications is interpreted as: 1) the content of communications relating to individual communications, and 2) includes components relating to individual communications, such as information that identifies the date and time of the communication, as well as the parties involved in the communication (names, addresses, etc.), and where the communication was sent from and received.
   Thus, the content (the text) and components (communicating parties, the dates and times the e-mail was sent and received, header information, etc.) fall under the category of the confidentiality of communications.
   Accordingly, the content or components of e-mails which providers become involved with through handling fall under the category of "the confidentiality of communications with which providers become involved with through handling."
2. Items that fall under the category of infringement
   The act of providers of filtering the content or components of e-mails which they become involved with during handling, detecting particular e-mails that correspond to the preset conditions and using them against the will of the communicating parties (e.g. blocking or discarding) is "to use against the will of the sender or recipient" the confidentiality of communications which providers become involved with during handling, and thus is interpreted to fall under the category of the infringement of confidentiality of communications.
3. Cases which do not against the will of the communicating party:

(1) A case does not fall under the category of the infringement of confidentiality of communications, if the consent of the communicating party is given for filtering the e-mail.
In this regard, regarding information for which the communicating parties have mutually left the confidentiality in the hand of the other's, the confidentiality will be released if the consent of one party of the communication is obtained. In this case, such an action is not interpreted to constitute theft. Specifically speaking, the confidentiality of information sent from the sender to the recipient of an e-mail (the text, subject, sender address, etc.) will be released with the consent of the other party.
On the contrary, regarding information that has been made confidential between the communicating parties, it is interpreted that the confidentiality will not be released unless the consent of the communication party who made the information confidential is obtained. Specifically speaking, regarding information that has not been sent to the recipient from the sender of an e-mail (i.e. the name, address and other data of the sender, in cases where they do not appear in the text) the consent of the party who made the information confidential (sender) is required.

(2) How to obtain consent

a. When providing filtering upon receiving an application from a user with the filtering of the initial setting turned off, it is generally deemed that effective consent exists.

b. Providing an initial setting with the filtering turned on cannot be generally deemed as appropriate, since prior comprehensive agreement by consideration and the like tend to involve an indefinite subject and range of consent (such as cases where the consent will be indefinite based on forecast, since the matter to be the subject of consent extends to future circumstances), and thus cases may be assumed where the consenting party has consented without understanding the subject and range of the consent.
Where, however, the following requirements are all met, we believe that we can interpret the filtering as being based on the

effective consent of the user, even if the initial setting is provided with the filtering turned on.

<Conditions for providing the initial setting with the filtering turned on>

1) It should be possible to change the details of consent (i.e. the change the setting) as desired from time to time even after the user has agreed to the provision of the filtering service;
2) Other conditions for provision shall be the same without regard to whether or not consent to the provision of the filtering service has been given;
3) The content of the filtering service shall have clearly defined limits;
4) It shall be reasonably presumed based on data such as the result of an inquiry survey that normal users will agree to the provision of the said service; and
5) The content and other matters relating to the filtering service shall be fully explained to users in advance (i.e. shall be explained according to a procedure that conforms to the explanation of the key issues specified in Article 26 of the Business Law).