Summary of Minutes of the 14th Meeting of the Round Table Conference on the Privacy of Information in the Telecommunications Service Sector

1 Date and time: October 12 (Tue) 2004 18:00 to 20:00

2 Location: Conference Room 1101 (11F), Ministry of Internal Affairs and Communications

3 Attendees:

(1) Members:	Otani, Kuwako, Tagaya (Acting Chairman), Tajima, Tezuka, Nakamura*, Hirukawa, Bessho, Horibe (Chairman), Matsui, Miki, Murakami, Yoshioka *Mr. Yutaka Nakamura, Director of the Legal Office, NTT DoCoMo Inc. has joined as a member in place of the retired member, Mr. Hirano.
(2) Ministry of Internal Affairs and Communications:	Aritomi (Director-General of the Telecommunications Bureau), Ezaki (Director-General of the Telecommunications Business Department), Oku (Director of Telecommunications Consumer Policy Division), Furuichi (Examiner), Fujinami (Assistant Director), Ikeda (Assistant Director)

4 Outline of proceedings

(1) Opening

(2) Exchange of Spam mail sender information

(3) Past discussions on penalties for unauthorized acquisition of information

(4) Closing

5 Major discussions

1) Exchange of Spam mail sender information

- We are studying a mechanism through which providers exchange

information on users who send e-mails that violate the display obligation of the Specific E-mail Law (spam mail sender information), where the provider takes measures against such users to suspend their use of e-mail. The names and addresses of such users will be made the subjects of exchange, while information on the details of their communications will not. In addition, suspension of use will be based on a declaration by recipients and providers that they will never monitor the content of communications of users.
The spam mail sender information possessed by each provider shall be updated upon regular exchange of information among providers. A database of spam mail sender information shall be kept by each provider.

- We cannot easily determine that spam mail sender information falls under the category of the confidentiality of communications, since it is not an individual form of traffic. On the other hand, it is debatable whether we can definitively judge that information confirming the fact that a spam mail has been sent does *not* fall under the category of the confidentiality of communications, and thus will not be protected. Eventually, it will be judged considering a balance between the interests of the parties concerned.
- The major issues are whether providers have uniform criteria for recognizing spam mail senders and whether the spam mail sender information that is to be exchanged is reliable enough for providers to reject subscription based on the information.
- Some may consider that the information on the receiving screen voluntarily provided by the recipient does not constitute communication handled by the provider. The private information which could be exchanged comprises the subscriber’s name and postal address, which cannot be identified from the receiving screen. However, providers can locate the name and postal address through the e-mail address of the transmission source shown on the receiving screen. In this sense, it can be said that providers are in potential contact with such private data when handling the above information.
- This may relate to the protection of personal information. Isn’t there

any possibility that users may suffer suspension of use when they have no reason to be treated as such due to wrong personal information, etc?

- Using a false identity in mails sent from cellular phones is technically difficult, and there may be little possibility of erroneous suspension. On the other hand, it is true that there do exist some problems with mails sent from personal computers. As it has been going on now, it would be good to secure the accuracy of determination of facts by making judgment based on two or more transferred e-mails. We should also discuss possible remedies in cases where false identity has been used.
- We are unsure that we can judge that spam mail sender information is unrelated to the confidentiality of communications. It would seem better to determine whether or not the exchange of spam mail sender information is a justified operational act, in order to cope with cases where it is interpreted that the information falls under the category of the confidentiality of communications.
- Even if a person is registered in non-paying users' information, he/she can receive the service so long as he/she pays the overdue amount. Moreover, he/she will be removed from the non-payer's list in a year, and will again be fully entitled to receive the service. Similar recovery measures may be necessary in the case of the exchange of spam mail sender information. The idea of having a spam mail sender submit a written pledge in advance is easy to understand, but the idea of having the sender pay money as collateral to a new provider to which he/she has moved, would appear difficult in terms of civil restrictions.
- We believe that the points of contention other than the confidentiality of communications, such as the fairness of use and the obligation to provide service, are issues that we will be able to solve as we proceed with our discussion once the relationship with the confidentiality of communications is properly defined.
- The exchange of non-paying users information was discussed in the 90's, and the stipulation regarding the exchange of non-paying users information was added to the personal information protection guideline, taking into consideration the request to carry out exchange without taking the information from providers. Since such past background may

be useful for the exchange of spam mail sender information, we would ask you to review the issue once again and discuss the questions that arise.

- We have to discuss fully whether the exchange of non-paying users' information and the exchange of spam mail sender information can be considered in the same way. However, spam mail sender information is not a core part of the confidentiality of communications and thus there is no need to request strict protection for it. Some cases may exist where the exchange of information may be allowed after deliberations.
- The exchange of spam mail sender information may be widely accepted if disadvantages are controlled to some extent by adding cautionary requirements.

2) Past discussions on penalties for unauthorized acquisition of information

- In the discussion for establishing the Personal Information Protection Law, the important view, presented by the Ministry of Justice, was that it was difficult to include provisions for direct punishment to doers regarding general personal information leaks. We need to keep on discussing the matter, including whether it is really difficult to do so. It seems OK if we limit the components to some extent. Just as in the case of the leak from SoftBank, we are now addressing such cases by punishing not the theft of information per se, but other behaviors, and thus it is true that the interests that should be protected by law are not actually being protected. We think that it may be possible to provide direct punishment specifications if conditions are satisfied.
- The stipulation regarding punishment for persons who leak personal information in the Personal Information Protection Law for governmental agencies encouraged local governments to stipulate punishment to wrongdoers in their own regulations.
- As discussions are taking place in society at large regarding the need for the protection of personal information, it seems that the policy of punishing leakers of information may be applied to the private sector.

- Stipulations regarding the protection of the confidentiality of communications accompanied by punishment for wrongdoers already exist in the telecommunications service sector.
- The purport of the Personal Information Protection Law for governmental agencies is to have stricter stipulations apply to governmental agencies than to the private sector, since they have no choice but to handle personal information. Then perhaps we can say that the telecommunications service, too, needs to handle personal information during the course of its business. However, it is different from governmental agencies in that users can choose providers.
- The Personal Information Protection Guideline has just been completed and it seems that it will never be too late to determine whether direct punishments are required after applying controls under the guideline.
- We believe that there has long been the necessity for provisions stipulating direct punishments.
- Some operators require that provisions for direct punishment be established.
- We admit that we should at least continue discussing the matter in some way. The schedule is should reach a definite conclusion by the year-end, but we would like to conclude this conference by recognizing that we have got the past discussions straight. Let’s continue our discussions in the future.

(End)