Study Group on Systems in Ubiquitous Network Society
First Meeting Proceedings Summary (Draft)

1 Date and Time: February 21, 2006 (Tue) 15:00-17:00

2 Location: 9th floor, Meeting Room 901, Ministry of International Affairs and Communications

3 Attendees (Honorifics omitted):

(1)Members

Chairperson HORIBE Masao (Chuo Law School); Vice-chairperson IBUSUKI Makoto (Ritsumeikan University School of Law); OHTANI Kazuko (The Japan Research Institute, Limited); KISHIGAMI Junichi (Nippon Telegram and Telephone Corporation); KOMUKAI Tao (InfoCom Research, Inc.); TAMAI Katsuya (University of Tokyo); TERADA Shinji (Index Corporation); HIRANO Susumu (Chuo University); BESSHO Naoya (Yahoo Japan Corporation); YOKOYAMA Tsunemichi (Attorney at law); WAKIHAMA Noriko (Yomiuri Telecasting Corporation)

(2)Secretariat (MIC)

Director-General TAKEDA of the Information and Communications Policy Bureau; Director KONDO of the Research Department, Institute for Information and Communications Policy

4 Proceedings:

(1) Speech by Director-General of the Information and Communications Policy Bureau

Director-General Takeda made opening remarks.

(2) Study Group Outline (Draft)

An outline of this study group was explained by the secretariat, based on Reference 1-1, and approved.

(3) Scheme of Open Meeting

A scheme to open the meeting to the public was explained by the secretariat, based on Reference 1-2, and approved.

(4) Appointment of Chairperson and Vice-chairperson

Horibe was elected Chairperson by mutual vote. Chairperson Horibe appointed Ibusuki Vice-chairperson.

(5) Meeting Procedure

The meeting procedure was explained by the secretariat, based on Reference 1-3.

(6) Key Issues (Draft)

The secretariat explained the draft key issues, based on Reference 1-4.

(7) Presentation by member: 1

Ibusuki brought up some issues on (1) spyware control and (2) introduction of IT into judiciary and legislative systems.

(8) Presentation by member: 2

Komukai brought up some issues on the use of personal information in the ubiquitous network society, such as automatic collection of identification information, based on Reference 1-6.

(9) Presentation by member: 3

Hirano brought up some issues on corporate monitoring of employees' internal e-mail by referring to judicial precedents in the U.S.A., based on Reference 1-7.

(10) Specific issues (Spyware)

The secretariat explained anti-spyware measures in U.S.A., including examples of definitions of spyware and the current situation of spyware, based on Reference 1-8.

(11) Q&A/Opinion Exchange

Q&A and opinion exchange were conducted. Key questions/answers and opinions are as follows:

- ○Illegality of installing information collection software on a user's computer to prevent illegal copying could be dismissed, considering the protection objective of the Copyright Law.
- ○In the United States, user consent is generally obtained in advance by displaying a user consent screen when collecting information from a user's computer for a service or support.
- ○The definitions of spyware could be roughly summarized in the four requirements presented by the Anti-Spyware Coalition (ASC), a US anti-spyware industry group.
- ○The definitions in the spyware control bills submitted to the US Congress were in accordance with the four requirements. These definitions seem to represent the industry groups' perspective. On the other hand, the definitions on the consumer side would be more comprehensive with less rigorous objectives.
- ○Recently, some point out bots as a more serious problem than spyware. Since operations differ between spyware and bots, discussions focused only on spyware could leave bots out of the control framework.
- ○Spyware will not be installed on a mobile phone in the present circumstances, but it may only be a matter of time. Meanwhile, there is a problem in that mobile phone services cannot move to open businesses, remaining within a closed network, due to excessive awareness of the security issues, including spyware.
- ○In practice, what types of software are recognized by anti-virus software as spyware is more important than legal definitions. It is likely that anti-virus software definition files would become the de facto standard.
- ○Situations where whether user consent has been obtained or not is critical are expected to increase as it is an issue related to both spyware and personal information protection. As the recent case of erroneous stock ordering clearly suggests, users' capacity to respond, e.g. handling of warning screens, is reaching a limit. How to obtain user consent needs to be discussed by taking into account the aspects of users' psychology and cognitive capacity.

(12) Future schedule

The meeting procedure was explained by the secretariat, based on Reference 1-9, and approved.