Demonstration Project on Utilization of Privacy Information such as Location Information

Report Summary

March 2018

NOMURA RESEARCH INSTITUTE, LTD.

Contents

1. Study outline

1. Background and objectives
   - Through case studies in Japan and abroad, demonstration using model cases, examinations at councils by experts, etc., our study examined the proper processing of privacy information such as location information for the purpose of balancing free distribution of data and privacy protection.
   - Demonstration use model cases where data collectors and service providers serve as one. Concern which is unclear as to which of the plurality of business operators the authority to use the acquired data and the responsibility of the processing of the data are unclear, who the notice is to the consumer, who to agree with. Based on these problems such as complaints and difficulty in finding opt-out recipients, our study examined data processing on location information etc. with consideration of privacy.

2. Main elements of study
   ① Study on issues concerning rules concerning processing of location information etc. of telecommunications carriers
      - Issue1：The rules of privacy protection related to data utilization of probe requests in EU etc.
      - Issue2：Investigation on rules for sharing and providing location information among multiple business operators
      - Issue3：Investigation on the evaluation of privacy risk accompanying the progress of IoT

   ② Model demonstration

3. Establishment of consultative council
   - A consultative council was established and met four times. The council consisted of seven experts in fields including privacy of communications, privacy protection, anonymization technologies, and telecommunications policy, and included as observers the secretariat of the Personal Information Protection Commission of Japan, telecommunications carriers, other interested bodies and Model demonstration cooperation company.

Council composition

Members *Study leader

- Ryoji Mori* Attorney-at-law, Eichi Law Offices
- Yuriko Inoue Professor, International Corporate Strategy Hitotsubashi University
- Ichiro Satoh Professor, National Institute of Informatics
- Katsumi Takahashi Executive Research Scientist, NTT Secure Platform Laboratories
- Shinji Terada Senior staff, Keio Research Institute at SFC ／ Executive Director, Mobile Content Forum
- Toshiro Hikita Senior Researcher, Toyota InfoTechnology Center
- Tatsuhiko Yamamoto Professor, Keio University Law School

Observers

- Secretariat of the Personal Information Protection Commission, Japan
- Telecommunications Carriers Association (TCA)
- Japan Data Communications Association
- NTT DOCOMO, Inc.
- KDDI Corp.
- Softbank Corp.
- NTT Broadband Platform, Inc.
- Narita International Airport Corporation
- Japan Airlines Co., Ltd.

Secretariat

- Second Telecommunications Consumer Policy Division, Telecommunications Business Department, Telecommunications Bureau, Ministry of Internal Affairs and Communications (MIC)
- Nomura Research Institute, Ltd.

Issue1：The rules of privacy protection related to data utilization of probe requests in EU etc. — Privacy treatment for data utilization service of probe request in Japan and EU

- Services that acquire and analyze location information of pedestrians and vehicles without obtaining consent using smartphone probe request exist in Japan and abroad. However, both of them are marketing operators, etc., and there is no examples of the telecommunications carriers.
- Each company carries out privacy measures including hashing of MAC address acquired by probe request.
- Meanwhile, in the EU, there are cases requiring for stricter response to anonymization such as resetting hash algorithm.
  - Since it is understood that the MAC address corresponds to personal data in EU, when collecting, it is usually necessary to notify / consent to the data subject.

Example of privacy treatment when using Wi-Fi marketing provider when use probe request (common to both domestic and international)

1. Implementation of MAC address non-identification processing (hashing etc.) and clarification of the facts
2. Definition of storage period of acquired information
3. Presentation of signs / stickers informing that information is being acquired
4. Presentation of opt out means
5. Presentation of privacy policy on company site (Usage purpose, totaling method, utilization technology, information providing destination etc.)

The case which an anonymization treatment was requested in EU

- **Blip Systems（Denmark）**
  - ✓ According to the correspondence such as "Hash MAC address immediately", "hash algorithm reset in 24 hours", etc., the provision of services without obtaining consent was approved
- **retency（France）**
  - ✓ France Data Protection Agency (CNIL) approved based on the point that the collected MAC address is anonymized and deleted within 5 minutes, the point that the storage period for aggregation is separated by 15 days, the point that the hash algorithm is updated every 2 weeks, etc.
- **JCDecaux（France）**
  - ✓ MAC address is partially truncated and salt (String for changing hash value) is added by hashing. However, since it was not reset and repeater analysis could be done, it was insufficient as anonymity, and CNIL did not give permission.

* All of the above cases provide a service for tracking position information of pedestrians and vehicles using smartphone probe request.

Issue1：The rules of privacy protection related to data utilization of probe requests in EU etc. — Types of elements of rules related to data utilization of probe requests

- The following items would be elements when using the probe request (Information transmitted by the terminal to connect to other equipment and network equipment) without clear consent of the person.
  Since each item is related to each other, it is necessary to pay attention to that rules are being examined together.

1. Notification method
   - Notification content
   - Means of notification

2. Purpose limitation
   - Whether to restrict the purpose of using probe data collection (Limited to statistical counting * etc.)

3. Data Minimization
   - Whether to limit the temporal and spatial range of probe data collection
   - How much anonymization is required

4. Opt out method
   - Whether to provide a valid opt-out method

※”Statistical counting” is used on WP247: Opinion 01/2017 on the Proposed Regulation for the ePrivacy Regulation (2002/58/EC)”

Issue2：
Investigation on rules for sharing and providing location information among multiple business operators
— Sample contracts and commentary on data processing between multiple business operators

- Sample contract
  - Samples of the clauses that might be considered and a commentary which is needed when concluding contracts on data processing related to location information etc. processed by telecommunications carriers are compiled.

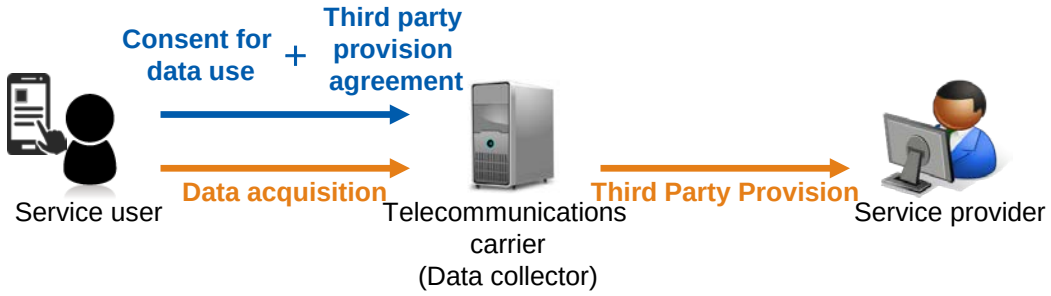
- Sample case
  - A case where a telecommunications carrier acquires and processes position information, etc. and provides it to a third party service provider (Case of provision to a third party) is basically based.
  - In addition, it explains the difference between cases where telecommunications carriers and service providers share location information etc. (Case of joint usage), and cases where service providers and telecommunications carriers acquire location information and the like (Case of multiple entities acquisition)
  - Based on acquisition (including multiple entities), provision to a third party and joint usage, it is assumed that obtaining 'specific and definite consent' from service users regarding acquisition, provision to a third party and joint use at the time of data collection.

Structure of the contract sample

Issue2:
Investigation on rules for sharing and providing location information among multiple business operators
— Case of obtaining consent regarding data processing between multiple business operators

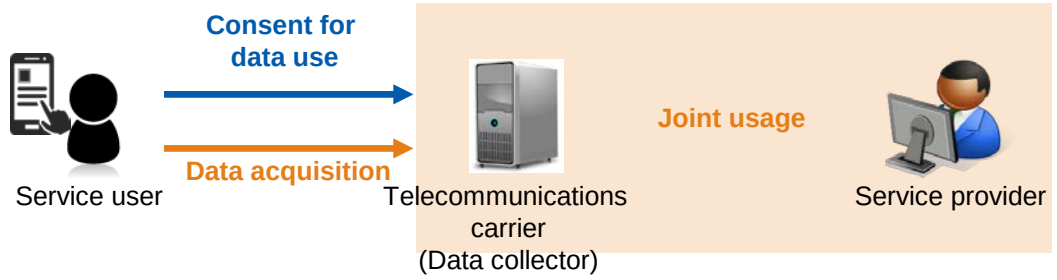
Case of provision to a third-party

- When the data collector acquires consent on data use, it is needed also obtain consent for third party provision.



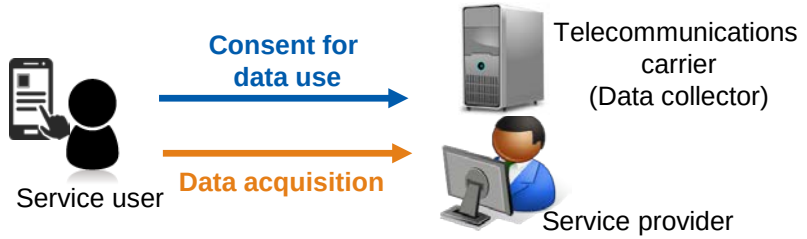
Case of joint usage

- The data collector and the service provider obtain consent to use the data based on the same purpose of use.



Multiple entity acquisition case

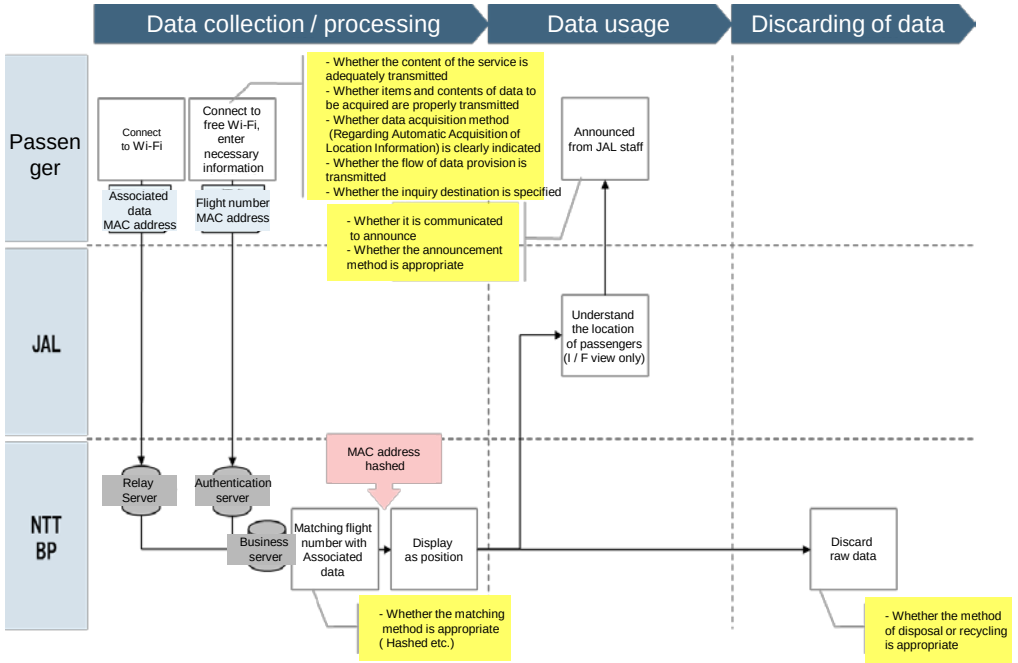
- The data collector and the service provider obtain consent for data use respectively.
- The purpose of use is not necessarily the same.



Issue3：Investigation on the evaluation of privacy risk accompanying the progress of IoT — Implementation of privacy impact assessment in model demonstration cases

- With the development of IoT, telecommunications carriers will provide services in cooperation with businesses in various fields. Accordingly, it is assumed that telecommunications carriers will be necessary to deal with the privacy problem which is hard to suppose in the extension of the conventional business. For this reason, privacy impact assessment was conducted for IoT related services using position information taken in model demonstration.
- Specifically, this study extract privacy risk from data flow with experts and decide treatment policy and evaluated the acceptability of service users through questionnaire survey.

Data flow and privacy risk



Privacy risk and Response policy

	Privacy risk	Treatment policy
Data collection / processing	✓Whether the content of the service utilizing the data is adequately transmitted (Contents and method of announcement)	✓Discriminate the current location of the passenger using the position information and the flight number information on the portal screen and make a necessary explanation ✓Make an appropriate explanation in the Terms of Service
	✓Whether items and contents of data to be acquired are properly transmitted	✓In the portal screen and the terms of use, clearly states that the information of the Wi-Fi access point the occupant last connected and the flight name entered by the consumer used
	✓Whether data acquisition method is clearly indicated (Especially automatic acquisition of location information)	✓Explain that the passenger automatically acquires the information of the Wi-Fi access point last connected and discriminates by using the MAC address in the usage agreement
	✓Whether the processing method of the acquired data is clearly indicated	✓Specify in the terms of service that data should be processed into a state unrelated to the person on the day of acquisition (MAC hashed hashed)
Data utilization	✓Whether the usage purpose of the data (application to announcement) to be acquired is adequately transmitted	✓Discriminate the current location of the passenger using the position information and the flight number on the portal screen and make a necessary explanation about announcing ✓Make an appropriate explanation in the Terms of Service
	✓Whether the flow of provision of data to third parties is adequately transmitted (Notice that NTTBP acquired and provided to Japan Airline)	✓The portal screen clarifies that NTTBP collects and provides it to JAL ✓Make an appropriate explanation in the Terms of Service
Data discarding	✓Whether the opt-out method or alternative way of protecting users is clearly indicated	✓The location information to be acquired is confined to the airport facility and clearly stipulated in the terms of service to process to a state unrelated to the person in one day
	✓Whether the method of data (Method, cycle, etc.)discarding is appropriate and clearly indicated to consumers	✓The location information to be clearly stipulated in the terms of service to process to a state unrelated to the person in one day
General	✓Whether the contact information is specified	✓Specify contact information for free Wi-Fi service and boarding guide service by portal screen and terms of use

Overview and summary of study

Purpose

- Verify items to be notified to consumers in acceptance and provision of providing location information using location information by providing location information acquired by a telecommunications carrier to another business entity.

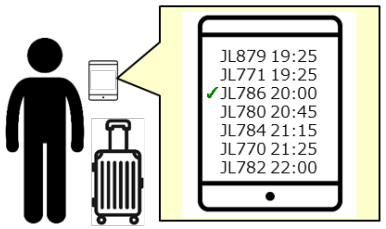
Study Contents

- During the demonstration period, we requested participation in a model case * for consumers on a specific flight of Japan Airlines at Narita International Airport Terminal 2.

≪ Image of demonstration participation flow ≫

Step1. Register boarding flight number

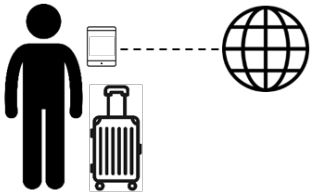
Register "flight number" when starting use of free Wi-Fi for study



User

Step2. Use the internet service

Internet service can be used freely until boarding

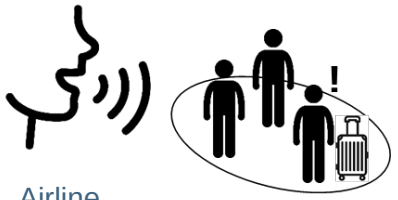


User Internet

Step3. Guide boarding

If customer isn't near the boarding gate when boarding time is approaching, check the customer location for each area and airline staff will guide on boarding

*It does not guarantee boarding



Airline Staff User

Result of the acceptability study	■ Answer that about **90%** of respondents **want to use as actual service** ■ Even in the absence of acceptability, only few respondents (less than 5% of the total) seem to be caused by the challenge to utilization of location information
Point out from the committee on the study result	■ It is a pleasure that consumers' acceptability was high. However, in this Model demonstration, **staff are presenting face-to-face explanations of service contents**, but **there is room for consideration as to how to notice to notify**. ■ Because **the Model demonstration was clear both in the service content and the required data**. Therefore it was easy for consumers to accept and also useful for business operators. **Depending on the service, it is not necessarily the case.**

* As a model case other than the above, for lending wheelchair users of Japan Airlines for specific flights, a portable terminal is attached to a lending wheelchair, and when a passenger is away from the boarding gate near the boarding time, an alarm is issued from the terminal I also demonstrated it.

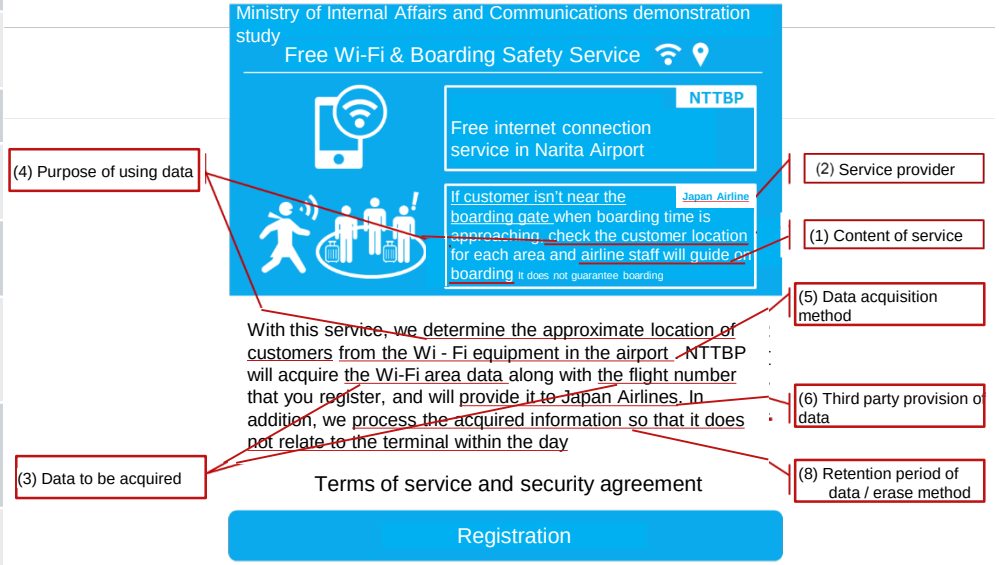
Content to be notified / consent to consumers

- When providing the location information acquired by the telecommunications carrier to another business provider and providing the service using the location information, 9 items were arranged as contents to be notified / agreed to the consumer

≪ Content to be notified / consent to consumers ≫

Content	Overview
(1) Content of service	• Outline of services to be provided
(2) Service provider	• Indicate the provider of the service • Describe when there are multiple providers
(3) Data to be acquired	• List data items and contents to be acquired
(4) Purpose of using data	• Specify the purpose of using the data concretely. If the purpose of use is different, specify it separately
(5) Data acquisition method	• Whether the terminal is communicating and acquiring, or by input by the service user, etc.
(6) Data provision to a third party	• Indicate the destination of the data. It is desirable to specify individually, but it is also possible to specify and indicate range
(7) User participation (Suspension of process etc.)	• Shows how to stop processing • If it is difficult, indicates that appropriate privacy protection measures have been taken
(8) Retention period of data / erase method	• Shows data retention period and deletion schedule
(9) Contact desk	• Describe the contact address (telephone number, mail address etc.) of the contact desk

≪ Correspondence with portal screen * in Model demonstration ≫



(7) User involvement and (9) contact desk were presented in detailed terms of use

Result of the acceptability study	■ Answer that about **80%** of respondents answered that **they understood services** which based on the utilization of location information through the portal ■ As **items to be notified beforehand in advance, "How long will it take" Location information will be acquired**
Point out from the committee on the study result	■ In order to help consumers understand the contents of services using location information received from another business entity, it is desirable **to post websites, posters, etc. showing the contents of the service additionally** ■ It is desirable to inform the **consumer of the precision in addition to the data items as contents to be notified to the consumer**

*When the participant first connects to the proof Wi-Fi network, the first screen displayed on the mobile terminal

3. Challenges and future developments

- Incorporation into industry group rules
  - The present study resulted, as a rule concerning the processing of location information etc. of telecommunications carriers, it has compiled a contract sample for processing of location information among multiple business operators and their commentary. These are expected to be taken over by trade associations in the telecommunications business field and to be used as a standard for processing location information.
  - The amended Personal Information Protection Act went into full effect on May 30, 2017. In conjunction with this, the “Guidelines on Personal Information Protection in the Telecommunications Business” also entered effect. It is hoped that industry groups and authorized personal information protection associations were formulated voluntary rules and personal information protection guidelines based on the details compiled for this study, and MIC need to organize initiatives to support these activities.

- Follow-up on rules on data processing in EU etc.
  - In this study, based on the discussions of the EU etc., the elements of the rule in the case of not obtaining clear consent of the person concerning the use of data such as the probe request, etc., have been arranged. There are few cases of using data such as probe requests by telecommunications carriers in Japan, and the needs are not clear. Therefore, although there is no immediate need to improve the rules, it is compiled to contribute to future consideration.
  - In EU, with the full enforcement of the General Data Protection Regulation (GDPR) on May 25, 2018, the task of formulating the data protection rule "draft privacy regulations" by telecommunications carriers It is being advanced. It is planned to review regulations concerning tracking etc. by Wi-Fi etc.
  - According to these reason, it is considered necessary to follow-up discussions of the EU etc. continuously, assuming that the need for utilizing data such as probe requests in the telecommunications business field has been clarified in Japan.