Proposal of a New Privacy Protection Scheme for the Data Subject on the International Cooperation Information Sharing Platform

Naonori Kato(✉), Haruo Takasaki, and Yosuke Murakami

KDDI Research Institute Ltd., Tokyo, Japan
{xan-katou, ha-takasaki, yk-murakami}@kddi.com

Abstract. A novel project called iKaaS (intelligent Knowledge-as-a-Service) was adapted as a Strategic Information and Communications R&D Promotion Programme (SCOPE), one of the projects funded by Ministry of Internal Affairs and Communications. This project aims an advanced knowledge-intensive platform that enables to provide and distribute the relevant information under strict consideration of privacy. This information distribution includes a cross-border one between EU and Japan, where privacy protection of the data subject is a major issue. To settle the privacy issues inside the project, DPEC (Data Protection and Ethical Community) was established as a governing organization for privacy. In this paper, we consider issues on the cross-border data distribution from the viewpoint of the legal system comparison between EU and Japan. As a result of the consideration, we introduce the governance framework of DPEC. Moreover, we clarify the issues to be discussed in the future cross-border data distribution and propose a privacy enhanced data protection scheme.

Keywords: Act on the protection of personal information · KaaS · Privacy · Cross-border data distribution · Big Data · Data protection

1 Introduction

Recently, "Big Data" or "IoT (Internet of Things)" have increasingly emerged as buzzwords in the field of network technology. This phenomenon means that any type of data has practical potential to be used in any field. A variety of approaches to data utilization have been tried both in research and in business. During this turmoil on the data processing, misuses of personal data have appeared as a serious social problem.

The experiment which National Institute of Information and Communications Technology (NICT) in Japan planned provoked an issue of an appropriate use of surveillance cameras[1]. In this case, the surveillance cameras collected the movies of

[1] See. Investigative report which was written by a third-party committee (Only in Japanese), http://www.nict.go.jp/nrh/iinkai/report.pdf. That concluded the experiment was no illegal, but needs explicit notices. NICT planned to use surveillance cameras to control streams of people in the station.

K. Giokas et al. (Eds.): eHealth 2016, LNICST 181, pp. 23–28, 2017.
DOI: 10.1007/978-3-319-49655-9_4

pedestrians at the station without any consents or notices. That is similar with Google street view case. The public announcement from NICT on the experiment provoked a social argument. This situation compelled NICT to establish a third-party committee and to publish its report. This report concluded the experiment was not illegal, but needed explicit notices, although NICT had planned to use surveillance cameras for control of people streams in the station.

In other case, the personal data disclosure which Japan Railway East (JR East) planned to the business partner induced an issue on the definition of "personal information"[2]. JR East sold the passengers' records to the third party without any consent from each passengers. JR East's public announcement to start this disclosure to the third party inflamed a social argument. This situation also imposed JR East to publish a report on the disclosure of passengers' records outside JR East. In this report, JR East didn't mention illegality of the disclosure. JR East planned to disclose chronical passenger boarding data after only removing names of the passengers, and leaving all other data as they were. This procedure faced severe social criticism because a passenger can be estimated by the disclosed chronical data.

Meanwhile, EU has shown constant concerns on data protection, and has recognized the data protection as a hot issue. In October 2015, the European Court of Justice declared invalidity of the Safe Harbour Decision. Under the promoting pressures for data utilization, we acknowledge the urgent clarifying the proper and legitimate sharing of the personal data.

The one hand "Big Data" is considered as "new oil", the situation to utilize data in the society is becoming complex more and more. The In this paper, we analyse.

2 Issues on the Information Sharing in the Society

On the information sharing platforms, a wide variety of data are exchanged and combined among a number of parties over the borders. We will discuss three big issues on the information sharing process. Each issue is described below.

2.1 Context-Dependent Values of the Information

A wide variety of data are exchanged and combined on the information sharing platforms. The iKaaS project aims to produce a service by creating new knowledge based on a combination of data among different industries, the combinations of which have not been imagined so far. Attempts to combine these various data open new possibilities of data utilization. However, a new combination of various data may reveal

[2] See. Investigative report which was written by a third-party committee (Only in Japanese), http://www.jreast.co.jp/information/aas/20151126_torimatome.pdf. This is the report about the disclosure of the data of Suica outside JR East. The third-party committee didn't mention illegality of the disclosure. JR East planned to disclose boarding history data on Suica, where only names of the card holder were removed. This procedure was criticized because a person who holds the Suica can be estimated by the boarding history data.

unexpected values. For example, some combination of data proved to cause privacy infringements which the platformer had not expected. A simple sensing data or statistical data that have not been treated as a privacy or personal information may trigger privacy invasion. The JR Suica case showed a card holder may be identified based on the combined boarding histories. The JR EAST had explained SuicaIDs (identifier of Suica service) had become irreversible by the number conversion. However, even in such a case, some researchers has pointed out it is possible to re-identify the holder. Also, individual living area of the holder can be almost uniquely estimated from the recorded histories of departure stations and arrival stations. Pseudonymised (including linkable anonymous data) or anonymized method for the data is not effective for preventing such re-identification trials. When we consider more complex context, we have to take into consideration more increased risks of privacy infringements.

When we review international situation on privacy protection, we clearly recognize discussions on privacy matters go deep in the future. Here we show two examples of ongoing discussions. One is the draft of General Data Protection Regulation[3], where "Personal data" is defined as "'personal data' means any information relating to a data subject". The other example is the draft: Consumer Privacy Bill of Rights Act of 2015[4], where "personal data" is defined as "In General— 'Personal data' means any data that are under the control of a covered entity, not otherwise generally available to the public through lawful means, and are linked, or as a practical matter linkable by the covered entity, to a specific individual, or linked to a device that is associated with or routinely used by an individual, including but not limited to—..". In both case, the definitions of personal data has wide meanings.

2.2 The Information Sharing Parties

If the data is processed only within individual party, it is not difficult to define the domain of data utilization. On the other hand, when we consider a situation where the information is shared among several parties, we point out two issues. The first issue presents difficulty of defining information sharing parties. It is unclear whether we are able to itemise all the parties which shares information at present or in the future. Failure of showing all the relevant parties violates against the following law requirements: requirements: in Act on the Protection of Personal Information[5] in Japan, article 17[6]

[3] See. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)/* COM/2012/011 final - 2012/0011 (COD)*/ http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:52012PC0011.

[4] See. Administration Discussion Draft: Consumer Privacy Bill of Rights Act of 2015 https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.

[5] See. Act on the Protection of Personal Information (translated in English) http://www.japaneselawtranslation.go.jp/law/detail_main?id=130&.

[6] (Proper Acquisition) Article 17 A business operator handling personal information shall not acquire personal information by a deception or other wrongful means deception or other wrongful means.

ordains "Proper Acquisition", and in EU Data Protection Directive[7], article 7[8] ordains "CRITERIA FOR MAKING DATA PROCESSING LEGITIMATE". The second issue is difficulty in defining the purpose of data processing. This difficulty opposes law requirements which demands other purpose than the four conventional purposes (collection, storage, usage, and disclosure) should be explicit and legitimate. However, through trials of combinations of data processing whose purpose is unpredictable, our project is expected to deliver a novel knowledge and service. In order for our project to be legally conformant, explicit informed consent is the only reasonable solution.

2.3 Cross Border Transfer

In EU Data Protection Direction, article 25[9] ordains cross border transfer of personal data. If a third country is to be assessed as an adequate level of protection, it must satisfy article 29. In this project, we plan to transfer data from EU to Japan, but Japan has not the adequacy. If the third country does not have the adequacy, it needs other options (including "SCC" (Standard Contractual Clauses), "BCR" (Binding Corporate Rules) or other international agreement like Safe Harbour agreement between EU and US). At present, Japan does not have international agreement with EU. In addition, both SCC and BCR are too difficult to be certificated for academic research projects. By the way, In EU Data Protection Direction, article 26[10] ordains "Derogations". When the data subject has given his consent to the proposed transfer without clear refusal, Japanese parties can transfer data from EU.

3 Proposal

To solve these problems, we would like to introduce the definition of stakeholders and the internal audit organisation "DPEC".

3.1 Definition of Stakeholders on the Processes

Conventionally, the scheme of the personal data transfer and utilization has been classified as four stages: data collection, storage, usage and disclosure (provision to a

[7] See. Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data http://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:31995L0046.

[8] Article 7 clarifies the conditions for consent to be valid as a legal ground for lawful processing.

[9] Article 25 1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.

[10] Article 26 Derogations 1. By way of derogation from Article 25 and save where otherwise provided by domestic law governing particular cases, Member States shall provide that a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2) may take place on condition that: (a) the data subject has given his consent unambiguously to the proposed transfer;.

third party). Many conventional services already obtain the user consent including the first three (from collection to usage) or all the four (from collection to disclosure) of the scheme. However, in our project, the conventional scheme fails to work, as in our project different parties are responsible for each data processing. We had to redefine each process and stake holder to acquire precise user consent through showing exact architecture of the service we are going to provide. Redefined stake holders are shown as follows.

Lead operator: The responsible operator for the iKaaS project in Japan.

System management operator: The responsible operator for the iKaaS platform (design, development, maintenance, operation and security issues etc.).

Data management operator: This operator will collect the information from the participants. It shall be as a responsible operator for collecting and preserving the information.

Data utilization operator: This operator will use the information preserved in the iKaaS platform. It shall be as a responsible operator for using the data.

We have also defined the process of obtaining user consents as follows.

1. Identify individual data to be collected (particle size of type and the data of the data).
2. When collecting the individual data, obtain the explicit consent from the data subject.
3. Define the way to combine what data for what purpose.
4. For the purposes shown above, obtain explicit consent from the data subject. In such consent acquisition process, obtain the consent of the clear opt-in type.

We would like to introduce this “Double informed consent” in order to strengthen user consents.

3.2 DPEC

The iKaaS project implements three use cases. One of the use cases in Japan will include field tests with citizens and procedures under ethical considerations. In the EU, the ethical issues are considered based on the EU data protection legal framework by the Project partners. Since there is no independent data protection authority in Japan at present 5 by contrast to the EU legal framework which has independent privacy commissioners, a self-regulated “Data Projection and Ethical Committee” (DPEC) has been set in the iKaaS Project. DPEC shall clarify legal protection and ethical treatment of personal information gathered and shared among iKaaS Consortium Partners for research and development through iKaaS Platforms, especially concerning the use case which needs ethical considerations, and also the cross-border applications.

DPEC shall draft a privacy policy and a written consent forms and other appropriate guidelines (called “privacy protection documents”) in accordance with existing Japanese governmental guidelines, laws and regulations protecting personal information in

Japan. DPEC shall timely review the privacy protection documents depending on the legal amendments by government authorities. DPEC shall monitor the implementation by iKaaS Project Partners of privacy protection documents for adequate treatment of personal information gathered through iKaaS platforms. In the event of infringement of personal information, DPEC shall promptly advise corrective measures to iKaaS Consortium Partners. DPEC shall consult as appropriate legal counsels for getting independent advices as to the privacy protection documents and these implementations.

In the actual evaluation cycle, DPEC shall review the applications from each project partner. The application process shall start in advance of collection, storage, usage and disclosure of the data (including personal data) in the project. The applications shall be reviewed by the factors[11].

4 Conclusion

In this paper, we have introduced the definition of stakeholders on the information sharing platform and internal audit organisation "DPEC". The range of each law was confirmed through comparative law study. Furthermore, our self-regulation provides higher quality of privacy protection beyond the required level by the law. Our self-regulation scheme has proved to be friendly to the consumer rights to privacy and personal data.

In the next step, we plan to demonstrate practical experiments with the actual data collecting from the data subjects. We carefully observe any issue which may arise in performing the actual operation of the platform.

[11] We have defined 14 factors.