Abstract

An information processing model and a set of risk identification methods for privacy impact assessment in an international context

Yuki Kuroda
Kyoto University, Japan
2023

This doctoral thesis aims to propose a more systematic method than existing methods for two steps of Privacy Impact Assessment (PIA): the step of describing the processing of information as a preparation for risk assessment and the step of identifying risks as a starting point for risk assessment, with a view to the application of PIA to international personal information processing. In particular, the primary purposes are to respond to the following three issues regarding PIA.

(i) What does "risk" in PIA mean?
(ii) What methods effectively describe the information processing subject to risk assessment?
(iii) How should risks be identified based on the described information processing?

Chapter 1 is an introduction describing the issues of this thesis and presenting the overall structure.

Chapter 2 is a background chapter, first introducing two legal systems related to PIA, privacy and personal information protection, with a brief history and current status of each in the world and Japan. Privacy has not been clearly defined, and many countries have no detailed rules on whether a particular event infringes on privacy. On the other hand, complex laws and guidelines have been established in each country for personal information protection. The relationship between the two systems is that although the two overlap, each exerts regulation independently, and there is a gap in the scope of protection. Next, the thesis provides a brief history and overview of the PIA. PIA, like other risk assessment methods, consists of several steps, and the two steps that this paper focuses on are the essential prerequisite steps for effective analysis and evaluation, which are the core of risk assessment.

Chapter 3 examines the description model of international information processing. As

a premise, since PIA deeply connects with law, it is proposed to refer to the legal syllogism, a standard of legal application, to model information processing. Based on the syllogism, it presents a model with three parts: Applicable Law, Facts, and Rule Application Results, and further, there are five subparts each in Facts and Rule Application Results (the basic description model) and a specific way of expressing the model by combining a flowchart and tables. The basic model is effective in the hypothetical case where laws of multiple countries are applied to the same information processing.

Chapter 4 proposes a detailed description model that expands on the basic model discussed in Chapter 3. Although the basic model rightly presents the basic framework of model construction, it cannot describe the complex activities seen in modern personal information processing. Therefore, while maintaining the three-part structure of the basic model, the thesis proposes a detailed model that can describe even complex information processing by expanding the number of subparts that constitute the Facts and Rule Application Results in parts from five to ten in the basic model. In the process, this thesis found that personal information processing can be summarized in a single sentence that aggregates the ten subparts from the perspective of law. This chapter compared this detailed model with the most sophisticated previous study (a description model proposed to address the EU's privacy protection regime (General Data Protection Regulation, GDPR)). The conclusion is that the model can describe the application of the GDPR to the same extent as the previous study and can also describe the application of rules other than the GDPR that it has not covered at all.

Chapter 5 proposes a new approach to the risk identification step based on the description models in Chapters 3 and 4. First, this chapter analyzes PIA guidelines published by government agencies in many countries to clarify the nature of the risks to be covered by PIA. The scope of PIA varies among documents. A typical example is that some guidelines only consider compliance checks with the personal information protection legislation of the country where the document originates. In contrast, many consider privacy violations a risk in addition to compliance with personal information protection legislation. On this basis, mapping was done to show that the scope of PIAs can include up to four distinctive areas. Second, analysis of the guidelines revealed differences regarding the models that lead to the realization of risks and what negative impacts should be incorporated in PIA. This leads to the proposal of a privacy risk model. Based on these observations and proposals, this chapter provides a set of risk identification methods for each privacy and personal information protection area, as described in Chapter 2. It concludes that the pair would be helpful based on hypothetical cases. This chapter also links the previous chapters' detailed description model and risk identification methods.

Chapter 6 summarizes the results of this thesis and its limitations.
The main results of this paper for three issues are as follows.

(i) It found no unified understanding of the scope of risks covered by PIA and shows that PIA can include up to four distinctive areas (the former half of Chapter 5).

(ii) It found that personal information processing from the perspective of law can be expressed in the elements constituting a single sentence. It constructed the description model according to these elements, which can be applied to the international processing of personal information (Chapters 3 and 4).

(iii) It presented the set of risk identification methods according to the nature of the risks identified in the first half of Chapter 5, presented a privacy risk-specific risk model, and showed how to integrate the identification methods with the description model presented in Chapters 3 and 4 (the latter half of Chapter 5).