A Study on Abusing Superior Bargaining Position in the Anti-Monopoly Act and Its Relation to the Act on the Protection of Personal Information in Japan

Kaori Ishii

A Study on Abusing Superior Bargaining Position in the Anti-Monopoly Act and its relation to the Act on the Protection of Personal Information in Japan

Kaori Ishii[1]

[1] Faculty of Global Informatics, Chuo University, Tokyo, Japan
kaoriish@tamacc.chuo-u.ac.jp

Abstract. This study discusses the intersection between the Act on the Protection of Personal Information (APPI) and the Anti-Monopoly Act (AMA) in Japan, by focusing on abusing superior bargaining position from platform operators. My analysis is based on examinations of the provisions and related guidelines of AMA, the relevant provisions of APPI, and comparisons between the two regulations. Based on these findings: (1) most of the types of abuse which the Guidelines on Abusing Superior Bargaining Position (ASBP Guidelines) presented by Japan Fair Trade Commission (JFTC) overlap with APPI provisions; (2) restrictions on abusing superior bargaining positions could play a specific role by applying itself to profiling activities which APPI might not effectively regulate. However, the possibility for indefinitely expanding the scope of "superior bargaining position" and the scarce experiences of administrative fines would be challenges for AMA. In addition, clarifying the theoretical reason to incorporate privacy and personal data protection into AMA would be a fundamental issue. Other than abusing superior bargaining positions, cooperation or conflict between anti-monopoly law and protection of personal information law need to be carefully examined depending on the situation, such as refusal of deal, and merger. While privacy and personal data must be the first priority in laws designed to protect personal information, competition law and other adjacent laws are increasingly significant. Studying them can offer a different perspective on the protection of personal information.

Keywords: Abusing superior bargaining position, Privacy, Personal information, Competition.

1 Introduction

Big data analytics, Internet of Things (IoT), and Artificial Intelligence (AI) have created tremendous amounts of global data flow which is rapidly changing the online world.

For instance, CISCO's survey estimates that annual global IP traffic will reach 4.8 ZB per year by 2022, or 396 exabytes (EB) per month [1].

Borderless data flow has gradually broken-down jurisprudence barriers. The more complicated the online world becomes, the more likely it is that information-related intersecting legal issues will increase. This tendency is applicable among data protection laws, competition laws, and consumer protection laws in relation to regulations on "platform operators." The definition of platform operators encompasses a wide range of service providers: online shopping malls, internet auctions, online flea markets, apps markets, search services, contents distribution services (image, video, music, e-book, etc.), booking services, sharing economy platforms, social networking services (SNS), video sharing services, electronic payment services, and so forth [2, p.2]. Deceptive data practices by these services or their users would simultaneously provoke infringements of consumer contract law, personal information protection laws, and competition laws. Cabinet Office, JFTC, and Consumer Affairs Agency in Japan, and other similar agencies have held expert meetings to launch new policy strategies designed to address legal issues raised by platform operators. One policy strategy, for example, was the enactment of the Act on Improving Transparency and Fairness of Transactions of Specified Digital Platform Operators, which passed the National Diet on May 27, 2020 [3].

Among a series of legal challenges, this paper focuses on one of the intersection between APPI and AMA. On December 19, 2019, JFTC released the "Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc." [2] They are the first guidelines which shed light on how infringements of personal information can be regulated by AMA. In principle, AMA is an economic law which aims to ensure sound competitive surroundings, not protect privacy and personal information. While APPI is better suited to protecting personal information, these types of data have started to affect legitimate competition as many kinds of personal data have been traded in digital markets.

Based on the above information, this paper overviews provisions of abusing bargaining position in AMA, JFTC Guidelines, and APPI provisions, then discusses the division of roles between AMA and APPI.

2 JFTC ASBP Guidelines

2.1 Abusing Superior Bargaining Position

On December 17, 2019, JFTC published the Abusing Superior Bargaining Position (ASPB) Guidelines. They are the first guidelines in Japan covering practices that relate to the processing of personal information.

Article 19 of AMA restricts "unfair trade practices." This term includes abusing a superior bargaining position defined in Article 2(9)(v) [4].

- (v) engaging in any act specified in one of the following by making use of one's superior bargaining position over the counterparty unjustly, in light of normal business practices:

- (a) causing the counterparty in continuous transactions (including a party with whom one newly intends to engage in continuous transactions; the same applies in (b) below) to purchase goods or services other than those to which the relevant transactions pertain;
- (b) causing the counterparty in continuous transactions to provide money, services, or other economic benefits;
- (c) refusing to receive goods in transactions with the counterparty, causing the counterparty to take back such goods after receiving them from the counterparty, delaying payment to the counterparty or reducing the amount of payment, or otherwise establishing or changing trade terms or executing transactions in a way disadvantageous to the counterparty.

If a platformer abuses their bargaining position toward a consumer by processing their personal data, that practice could be deemed an unfair trade practice based on "otherwise establishing or changing trade terms or executing transactions in a way disadvantageous to the counterparty" under Article 2(9)(v)(c) of AMA.

In order to regulate a platform operator's ability to abuse bargaining power relating to the processing of personal information against a consumer, the scope of definitions must be clarified. First, the ASBP Guidelines state that a "'digital platform' has the characteristics of providing third parties with online platforms for various services by using information and communication technologies and data in a way which creates multi-sided markets with multiple user segments and a so-called indirect network effect." [2, p.2] A "digital platform operator" encompasses a broad range of businesses, such as online shopping markets, sharing economy platforms, and social networking services (SNS). Second, ASBP Guidelines cover "personal information, etc." While "personal information" in these guidelines are identical to Article 2(1) of APPI, which means "information relating to a living individual," ASBP Guidelines also cover "etc." which refers to "information relating to an individual except for personal information [2, p.3]." This is intended to cover a broader scope of information than APPI.[1] Third, "consumer" refers to an individual, but not one who use the service provided as a business or for business purposes [2, p.3].

2.2 Exploitative abuse against a consumer

Interpretive challenges exist when addressing exploitative abuse against Japanese consumers. Regulations on superior bargaining power have been primarily designed to protect small and medium-sized enterprises. Therefore, the scope of "counterparty" has not necessarily consumer-protection into consideration [6, pp.190-191]. AMA does not explicitly restrict some abuses, such as those where consumers are directly harmed by

[1] The term "personal data" in ASBP Guidelines covers the same scope of APPI. Under APPI, "personal information" and "personal data" have different definitions. The latter means personal information constituting a personal information database etc. under Article 2(6) of APPI, which is narrower than the former [5].

unfair terms or conditions being imposed on them; this is present in other regulations, such as Article 102 of the Treaty on the Functioning of the European Union.

Although the term counterparty itself does not theoretically exclude consumers, exploitative abuse against consumers is increasingly problematic in platform operator services, and protection of personal information is often compromised by abusing a superior bargaining position.

ASBP Guidelines may be informed by this background information when they allow that "counterparty (in continuous transactions)" includes consumers. ASBP Guidelines say "The personal information, etc. includes all information related to the individual consumer, such as the consumer's personal attributes and activities. Such information is used in the digital platform operator's businesses and thus has economic value. Therefore, when it is found that consumers provide personal information, etc. in exchange for the use of the services provided by a digital platform operator, then such consumers obviously fall within the definition of a "'counterparty (in continuous transactions)' of the digital platform operator" [2, pp.4-5].

2.3 Types of abuse of a superior bargaining position

Regarding what would constitute "unjustly in light of normal business practices," ASBP Guidelines explain that "abuse of a superior bargaining position is determined on a case-by-case basis from the viewpoint of the maintenance and promotion of fair competitive order. "Normal business practices" here are acceptable in terms of the maintenance and promotion of fair competitive order." [2, p.6]

In order to clarify illicit activities, ASBP Guidelines show several examples of abuse of a superior bargaining position [2, p.6-11].

The first example is unjustifiable acquisition of personal information, defined by breaking down three patterns: (1) acquiring personal information without stating the purpose of its use to consumers on its webpage or in any other ways; (2) acquiring personal information against consumers' intention beyond the scope necessary to achieve the purpose of use[2] ; (3) acquiring personal data without taking the precautions necessary and appropriate for safe management of personal information; (4) causing consumers in continuous use of services to provide other economic information, such as personal information, beyond that required for the use of services.

Second, the guidelines address unjustifiable use of personal information. According to ASBP Guidelines, the issue will arise "if a digital platform operator provides "information relating to an individual except for personal information" from consumers in order to make a third party collate "information relating to an individual except for personal information" acquired from consumers with other information and used for the purpose of causing a disadvantage for consumers" [2, p.10]. This example would cover profiling, which is discussed in the next section.

---

[2] For instance, this is exemplified by a case that a digital platform operator acquires gender and occupation information from consumers beyond the scope necessary for the sale of goods without obtaining the consumers' consent.

The second type is divided into two patterns: (1) using personal information against consumer intention beyond the scope necessary to achieve the purpose of use; (2) using personal data without taking the precautions necessary and appropriate for the safe management of personal information. Pattern (1) includes not only processing personal data beyond its original purpose, but also providing personal data to a third party without obtaining the consent of the consumer concerned.

2.4 Sanctions

Abusing a superior bargaining position in transactions constitutes a violation of AMA, which is subject to a cease and desist order under Article 20 and administrative fines that must be paid to the national treasury. The surcharge is an amount equivalent to one percent of the enterprise's sales to the counterparty to the violated act under Article 20-6. Administrative fines were introduced in the 2009 amendment of AMA.

3 APPI

3.1 Overview of the APPI

APPI is one of the Japanese Acts on the Protection of Personal Information enacted in 2003.[3] APPI obligates businesses handling personal information[4] to comply a set of duties as below [5][5]:

- Specifying a purpose for use (Article 15): Specifying the purpose for the use of personal information as explicitly as possible when handling personal information is required;
- Restriction to handle personal data beyond the original purpose (Article 16): Handling personal information beyond the originally specified purpose is prohibited without obtaining an individual's consent in advance;
- Appropriate collection (Article 17): Collecting personal information by deceit or other improper means is prohibited;
- Notification of a purpose or purposes for use when collecting the personal information (Article 18): Promptly notifying the individual of a purpose or purposes for use when collecting personal information is required;

[3] The other acts include Act on the Protection of Personal Information Held by Administrative Organs, Act on the Protection of Personal Information Held by Independent Administrative Institutions.

[4] This refers to someone handling a personal information database etc. for business use (Article 2(5)). A "personal information database etc." roughly means a systematically organized collective body of information comprising personal information (Article 2(4)).

[5] APPI tentative translation was partially altered to make the provisions clearer.

- Accuracy of personal data (Article 19): Striving to keep personal data accurate and up to date is required and immediately deleting personal data when its use has become unnecessary.
- Security of personal data (Articles 20-22): Taking necessary and appropriate measures for the security control of personal data such as preventing the leakage, loss, or damage of handled personal data is required. Measures include supervision over both employees and trustees;
- Restriction on providing personal data to a third party (Article 23): Providing personal data to a third party without obtaining an individual's consent in advance is prohibited.
- Restriction on providing personal data to a third party in a foreign country (Article 24): Providing personal data to a third party in a third country is prohibited except for a case fulfilling the stipulated requirements.

Other than these duties, businesses handling personal information are required to keep a record on a third party provision (Article 25), to confirm specified matters when receiving personal data from a third party (Article 26), and to make identified items of retained personal data public (Article 27). An individual has the right to access, correct, and to cease handling of their retained personal data (Articles 28-30).

One characteristic which defines APPI is its definition of personal information. APPI differentiates "personal information," "personal data," and "retained personal data," depending on the duty concerned. This is to prevent excessive extension of duties. The most fundamental definition is "personal information," which is defined as information relating to a living individual (Article 2(1))[6]. It includes information which can be easily collated with other information and thereby identify a specific individual (Article 2(1)(i)).

APPI established the Personal Information Protection Commission (PPC) by amendment in 2015, and it underwent a subsequent amendment in 2020. The amendment made in 2020 includes clear prohibitions regarding the inappropriate use of personal data, strengthened restriction of conditions that allow personal data to be provided to a third party, and the creation of requirements regarding notifications after a personal data breach [7].

PPC has supervising powers including requiring a report, conducting an onsite inspection (Article 40), issuing guidance and advice (Article 41), and issuing recommendations and orders (Article 42). A business handling personal information which violated an order by PPC would be punished by imprisonment with labor for not more than six months or a fine of not more than 300,000 yen (Article 84).[7] However, enforcement

[6] More detailed definition is provided in Article 2(1)(i)-(ii).

[7] Other than Article 84, if an operator handling personal information, its employee, or a person who used to be such a business operator or employee has provided or exploited personal information database etc., for the purpose of seeking their own or a third party's illegal profits, they would be punished by imprisonment with labor for not more than one year or a fine of not more than 500,000 yen (Article 83).

activities by PPC are moderate; it has not yet issued an order,[8] so penal sanctions under Article 84 have not been imposed. The amount of fine as per Article 84 was doubled by the 2020 amendment, but the date of enforcement would be within two years of the promulgation.

3.2 Rikunabi scandal

Since July 2019, the Rikunabi scandal has shaken public trust. This scandal involved Recruit Career wrongfully handling job seekers' information [8, 9]. Recruit Career is a large platformer service provider for both job seekers and client companies. It had been operating a platform called Rikunabi which provided a wide range of employment information. Recruit Career admitted that it made predictions about job-seeking students' odds of declining job offers and sold the data to 38 companies without obtaining proper permission from the candidates. This was done through the Rikunabi DMP Follow service, which was terminated on August 5th, 2019.

Recruit Career stated that it started selling students' data after March 2018, but only to clients who agreed not to use it to make a hiring decision. It explained in its privacy policy that it provided the information to client companies to support hiring activities, but also denied that such information would be used for a hiring decision. If client companies had used the purchased scores for hiring decisions, students' opportunities to obtain formal job offers would have been seriously distorted. The usages of data by client companies are still unknown.

PPC issued administrative recommendations and advice regarding this case in August 2019. The statements to Recruit Career indicated that it had lacked necessary security measures and fulfillment of requirements to provide personal data to third parties [10]. In December 2019, PCC advised companies which purchased data from Recruit Career that they needed to appropriately inform the involved individuals of the purpose of use for their personal data and also properly take control over trustees [11]. The data of around 26,000 individuals was subject to PCC supervision.

On another note, this case has provoked profiling issues. Profiling is regulated under the European Union's General Data Protection Regulation (GDPR) [12] and is defined as "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements" (Article 4(4) of GDPR). According to GDPR, a data subject has the right to object to processing of personal data concerning them, including profiling (Article 21 of GDPR). A data subject also has the right not to be subject to a decision based

[8] An order would be made when a business handling personal information has ignored a recommendation issued by PPC (Article 42(2)). If there is a need to take urgent action due to an event that seriously harms an individual's rights and interests, PPC is authorized to make an imminent order to a business handling personal information (Article 42(3)).

solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects them (Article 22 of GDPR). It seems plausible that these provisions could be applied to the Rikunabi case if a similar case took place in Europe. If companies used the scores for their selection processes, that represented a serious infringement of job seekers' right to make decisions about their lives. Calculating the possibility of declining a job offer using AI technology represents a typical case of processing of personal data to evaluate certain personal aspects.

The Rikunabi scandal only affected those in Japan and APPI does not explicitly stipulate provisions on profiling. However, the APPI amendment in 2020 has introduced restrictions on inappropriate use of personal information, and to strengthen requirements regarding providing personal data to a third party. Administrative fines were not introduced in APPI in the next amendment.

4 Discussion

The following knowledge can be gained from comparing the APPI and ASBP Guidelines.

First, most of the types of abuse covered by the ASBP Guidelines overlap with APPI provisions. Acquiring personal information without stating the purpose of use in ASBP Guidelines constitutes a violation of Article 15, which requires that the purpose of use be specified. Acquiring personal information beyond the scope necessary to achieve the purpose of use could constitute a violation of the same provision, and acquiring personal data without safe management constitutes violation of security of personal data (Articles 20-22). Only practices causing consumers to provide other economic interests, such as personal information, in addition to the data already provided in exchange for the use of services would be a specific example of abusing a superior bargaining position. If the purpose of use is properly specified, collecting personal information is not legally restricted under APPI. Therefore, if collecting additional personal information is inappropriate in the context of service provision concerned, ASBP Guidelines would be effective. The issue is that concrete examples have not been clarified.

Similarly, unjustifiable uses of personal information under ASBP are covered by APPI. Using personal information against the intention of consumers beyond the scope necessary to achieve the purpose of use constitutes violation of the restriction against handling personal data beyond the original purpose (Article 16 of APPI) as well as restriction regarding providing personal data to a third party (Article 23 of APPI), while using personal data without the safe management constitutes violation of personal data security (Articles 20-22). Regarding this, the 2020 APPI amendment has introduced restrictions on the inappropriate use of personal data and strengthen conditions on providing personal data to a third party, which will broaden restrictions of using personal information. The overlap between ASBP Guidelines and APPI would therefore increase.

In the context of restricting the inappropriate processing of personal information, both APPI and AMA have similar perspectives. The purpose of the ASBP provisions

under AMA are to restrict the infringement of freedom of the trading party, which includes the consumer as an individual. APPI aims to protect the personal information of an individual. Both laws could overlap concerning the protection of individuals in terms of handling personal information.

APPI is surely better suited for protecting personal data, but if it proves difficult for APPI to handle the problem, then AMA may address the new challenge.

Attention should also be drawn to the issue of profiling. ASBP Guidelines mentioned a case, for example, where a digital platform operator provides data other than personal information to a third party in order to produce personal information; this is done by collating information with other data, and can disadvantage consumers. This could be considered a profiling issue. In addition, the Rikunabi scandal could have been addressed by ASBP Guidelines, which interpret Article 2(9)(v) of AMA. In this case, Recruit Career was a platform operator, job applicants were counterparties, and the former party had a dominant position over the latter party. Recruit Career inappropriately combined, analyzed, and provided the applicants' data to client companies, which may have caused unfair hiring decisions for applicants.

Although PPC issued formal recommendations and advice to Recruit Career and also issued advices to other involved companies, APPI does not explicitly stipulate profiling provisions, and PPC does not have the authorization to levy administrative fines. Under AMA, an act falling within Article 2(9)(v) is subject to not only cease and desist order under Article 20, but also administrative fines under Article 20-6. This is just one example of how AMA could cover the shortages of APPI.

While AMA would be effective in some cases, there are also challenges. One is that the scope of ASBP which covers inappropriate processing of personal information could expand indefinitely. In the context of a relationship between a digital platform operator and a consumer, the former is deemed to have superior bargaining power against the latter in most cases as a consumer is compelled to accept the terms of use to become a user of the platform service.[9] "One's superior bargaining position over the counterparty" under Article 2(9)(v) of AMA would not be an effective limitation to define the scope. Another complication would be the limited experience of applying administrative fines. Administrative fines due to having abused superior bargaining positions have only been imposed on enterprises in five cases during 2011-2014; all of them are still in dispute [6, p.123]. No administrative fine based on ASBP has been imposed since 2014, meaning that experience in applying administrative fines due to ASBP is also limited.

Moreover, as a fundamental issue, the theoretical reasons behind why legal rights falling within the sphere of human rights, such as privacy and personal data protection,

[9] ASBP Guidelines state "A digital platform operator has a superior bargaining position over consumers who provide personal information, etc. when the consumer, even though suffering detrimental treatment from the digital platform operator, is compelled to accept this treatment in order to use the services provided by the digital platform operator." [2, p.4-5] This condition is applied to most cases between a digital platformer and a consumer transaction when personal information is a subject of trade.

could be incorporated into economic law needs to be clarified.[10] In this regard, the ASBP Guidelines state, "If services are provided to consumers in the manner which violates APPI, they are interpreted as not having the minimum quality of service level, thereby such services provided for profit are harmful to consumers" [2, p. 6, 10].

"Quality of service" could encompass many categories of value if a lack of such value compromises consumer interests. Privacy and personal data protection are surely included in the categories. However, it should be noted that AMA clearly stipulates its purposes as "to promote fair and free competition, stimulate the creative initiative of enterprise, encourage business activity, [and] heighten the level of employment and actual national income" (Article 1 of AMA). In contrast, privacy and personal data protection aim to ensure the peace of mind of each individual, which is not listed as the purposes of AMA. While AMA has the potential to shield consumers from various kinds of harm, it has an inherent limitation due to the AMA purposes. In order to avoid blurring the scope of law, AMA should carefully ensure that privacy and personal data protection are incorporated into its application to the extent possible.

5 Conclusion

This paper dealt with the division of roles between APPI and AMA, in the context of ASBP, relating to digital platform businesses.

The above discussions indicate that: (1) most types of abuse under ASBP Guidelines presented overlap with APPI provisions; (2) restrictions on ASBP could play a specific role by applying itself to profiling activities that might not be effectively regulated by APPI. However, the possibility for indefinitely expanding the scope of superior bargaining positions and the small amount of experience regarding administrative fines would be challenges to AMA regulation. In addition, clarifying the theoretical reason to incorporate privacy and personal data protection into AMA would be a fundamental issue.

While privacy and personal data must be protected primarily by laws regarding the protection of personal information, competition law and other adjacent legal fields are increasingly significant. These fields can offer a different perspective on how laws can protect personal information.

Other than ASBP, interplay between laws on protecting privacy, personal information, and competition laws arise in cases of refusal to deal, and mergers. The former would involve personal data portability, and the latter raises questions regarding whether privacy could be incorporated into the competition parameter.

---

[10] *See* Ohlhausen, M.K., Okuliar, A.P.: Competition, consumer protection, and the right [approach] to privacy. Antitrust Law J. **80**(1), 121–156 (2015). *See also*, Averitt, N.W., Lande, R.H.: Using the 'consumer choice' approach to antitrust law. Antitrust Law J. **74**(1), 175–264 (2007); Costa-Cabral, F., Lynskey, O.: Family ties: The intersection of data protection and competition law in EU law. Common Mkt. Law Rev. **54**(1), 11–50 (2017).

Unlike from ASBP, the requirements of AMA and APPI conflict in cases of refusal to deal. If JFTC orders an enterprise to allow competitors to access their data, APPI could be violated since it prohibits a business from providing personal data to a third party without an individual's consent. Interests protected by both laws should be adjusted in this case. As another example, APPI is not applicable in cases of business succession. Article 23(5)(ii) of APPI allows providing personal data to a third party as a result of the succession of business in a merger or otherwise. APPI cannot restrict providing personal data even if personal data might be compromised by a merger. AMA would be expected to protect personal data by incorporating its value into competition parameters[11].

Cooperation or conflict between AMA and APPI needs to be carefully examined depending on the situation.

6 References

1. Cisco Visual Networking Index: Forecast and Trends, 2017–2022 White Paper (2019). https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/white-paper-c11-741490.html#_Toc484813971
2. Japan Federal Trade Commission. Guidelines Concerning Abuse of a Superior Bargaining Position in Transactions between Digital Platform Operators and Consumers that Provide Personal Information, etc. (2019). https://www.jftc.go.jp/en/pressreleases/yearly-2019/December/191217DPconsumerGL.pdf
3. House of Councillors, the National Diet of Japan. An Act on Improving Transparency and Fairness of Transactions of Specified Digital Platform Operators (2020), (in Japanese). https://www.sangiin.go.jp/japanese/joho1/kousei/gian/201/meisai/m201080201023.htm
4. Act on Prohibition of Private Monopolization and Maintenance of Fair Trade (Act No. 54 of April 14, 1947). https://www.jftc.go.jp/en/legislation_gls/amended_ama09/index.html
5. Amended Act on the Protection of Personal Information (Tentative Translation). https://www.ppc.go.jp/files/pdf/Act_on_the_Protection_of_Personal_Information.pdf
6. Shiraishi, T.: Textbook on Anti-Monopoly Act, 8th edition. (2018). (in Japanese).

[11] The JFTC Guidelines to Application of the Antimonopoly Act concerning review of Business Combination (latest revision Dec. 17, 2019) shows how to assess the importance of data, by exemplifying a case when Company A has material input goods, such as data, and enters into a conglomerate business combination with Company B. The factors taken into consideration are: (1) what kind of data are held or collected by Company B; (2) how many data are held and how many data are collected daily by Company B from how wide an area; (3) how frequently does Company B collect data; (4) how many data are held or collected by Company B related to the improvement of the service provided by Company A in the product market. It is also considered how advantageous are the data held or collected by Company B as compared with the data available to the competitor (Company X) in the product market of Company A from the above perspectives (1) to (4). *See* Japan Federal Trade Commission. Guidelines to Application of the Antimonopoly Act concerning review of Business Combination (2019), https://www.jftc.go.jp/en/legislation_gls/imonopoly_guidelines_files/191217GL.pdf, p. 57. Though these factors do not directly affect the abuse of the superior bargaining position of a company to a consumer, they could be applied to a merger of companies profiting by handling personal information.

7. Personal Information Protection Commission. Amendment of the Personal Information Protection Act. (2020). (in Japanese). https://www.ppc.go.jp/news/press/2020/200612/
8. Asahi Shimbun. Recruit Career sold student data to firms without explicit consent (2019). http://www.asahi.com/ajw/articles/AJ201908020059.html
9. Asahi Shimbun. Rikunabi scandal highlights risks of exploitation of personal data (2019). http://www.asahi.com/ajw/articles/AJ201908130019.html
10. Personal Information Protection Commission. Recommendation, etc., under Article 42(1) of APPI (2019), (in Japanese). https://www.ppc.go.jp/files/pdf/190826_houdou.pdf
11. Personal Information Protection Commission. Corrective Measures under APPI (2019), (in Japanese). https://www.ppc.go.jp/files/pdf/191204_houdou.pdf
12. European Union. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal L 119, 1–88 (2016).