Journal of Korean Law | Vol. 17, 1-32, December 2017

The Limitations on the Use of Big Data Pursuant to Data Privacy Regulations in Korea*

*Jeong Yeol Choe,** Doil Son,*** and Sejin Kim****

Abstract

This study provides an overview of the current big data industry and regulatory parameters in Korea. It also makes policy and legislative recommendations for stimulating the big data industry, while preserving a balance between industry growth and the privacy of data subjects. For this purpose, we begin by reviewing privacy legislations from the European Union, the United States, and Japan. We also present domestic and overseas data breach cases. Further, we study relevant Korean court precedents and Korean privacy legislations to pinpoint obstacles to the promotion of big data under the current legislative regime.

South Korea's thorough privacy protection regulations essentially rival those of Europe. As of 2017, key privacy policy legislations applicable in Korea are given under the Personal Information Protection Act, the Act on Promotion of Information and Communications Network Utilisation and Information Protection, etc., and the Act on the Use and Protection of Credit Information, etc.

Because Korean privacy legislations define "identifiability" vaguely, businesses that employ big data technology face uncertainty about how to comply with various statutes and regulations, and this uncertainty restricts their production and use of big data.

Korean privacy legislations generally require personal information processors to acquire opt-in consents from data subjects to collect, use, and give third parties personal information. As a result, acquiring advance opt-in consents is necessary to generate big data from information that contains personal information.

Legislative direction that stimulates the big data industry must strike a fine balance between the constitutional rights to privacy and consumers' rights (i.e., the data subject of collected personal information) and the property rights of companies that own such information (i.e., big data companies). On the one hand, legislative changes extracting one-sided concessions from individuals about their privacy will likely be met with public resistance. On the other hand, continuing with laws that hamper the growth of the big data industry will undoubtedly

* The authors would also like to acknowledge the hard work of Woo Rim Lyou, a foreign attorney at Yulchon, for his support and assistance in writing this article.

** Partner, Head of Intellectual Property Practice Group, Yulchon LLC.

*** Partner, Co-Chair of Technology Practice Team, Yulchon LLC.

**** Attorney, formerly at Yulchon LLC.

sideline Korea from the fourth industrial revolution. Hence, scholars, legislators, and legal professionals must explore comprehensive measures that reconcile these two perspectives.

KEY WORDS: *Anonymisation, Big Data, Big Data Guidelines, Cross-Border Transfer, Data Privacy, De-identification, M&A and Data, Opt-in and Opt-out Consent, Outsourcing, Publicly Available Data, Re-identification, Third Party Provision*

Manuscript received: Doc. 23, 2017; review completed: Nov. 23, 2017; accepted: Dec. 1, 2017.

Introduction

The financial industry was among the first industries in Korea to embrace big data. For instance, Shinhan Card, a major credit card company, unveiled a big data centre in 2013. Subsequently, Shinhan Card released a product development system called "Code 9" (a product development system similar to "Sally," an individually customisable service) using its big data platform – which boasts 200 million approvals per month, 22 million customers, and 2.7 million branches. Code 9 categorises users into groups that share similar consumption patterns. Kakao Bank, which was established by Kakao,[1] the nation's largest messenger communications network with 42.74 million subscribers,[2] was launched on July 27, 2017 as

1) *See* Kakao Corp., *Kakao Corporation and Subsidiaries: Half-Year Financial Report for 2017*, KAKAO CORP., Aug. 14, 2017, https://www.kakaocorp.com/ir/referenceRoom/regularReports. (Follow "Download" under "Half-Year Financial Report for 2017.") This website describes the corporate background of Kakao Corp., which can be briefly summarised as follows: Kakao was established in 1995 under the company name Daum Communications ("Daum"), which provided the first ever email and web portal services in South Korea under Hanmail and Daum, respectively. In October, 2014, Daum merged with Kakao and the name of the corporation changed to Daumkakao, and as of October, 2015, the company name changed back to Kakao once again. Along with its subsidiaries, Kakao currently conducts business operations in the areas of communications (*e.g.*, Kakao Talk, Daum Mail, and Kakao Story), content platforms (*e.g.*, Kakao Page, Kakao Music, and Kakao TV), FinTech (*e.g.*, Kakao Pay), and gaming (*e.g.*, Kakao Game and Kakao Taxi).

2) Kakao Corp. *2nd Quarter 2017 Results*, KAKAO CORP., Aug. 10, 2017, https://www.kakaocorp.com/ir/referenceRoom/earningsAnnouncement?lang=en. (Follow "Presentation" under "Q2 2017 Kakao Earnings.")

an internet-based bank without any branches. Kakao Bank announced that it would use big data to establish and design a precise credit rating system. Subsequently, the bank surpassed one million subscriptions within a mere five days of its launch. As of September 11, 2017, Kakao Bank had two million standard transaction accounts and collected over one trillion Won in deposits and savings, earning the commendation that it had opened a new era of FinTech.[3)]

The public sector has also indicated interest in big data: in the past three years, the City of Namyangju (of Gyeonggi-do province) has announced that it will analyse big data on illegally parked vehicles to develop a map that marks areas where illegal parking is common. City officials will use this map as a reference to enforce parking regulations systemically, as well as in deciding where to install security cameras. In addition, Seoul's Gangseo-gu district office has announced that it will start conducting "pre-consultations for the analysis of big data" and will then develop a system for policy formulation through big data, starting in September 2017. Under this policy, any key policies that have annual operative costs of 100 million Won (approximately USD 90,000), employ personnel of three or more individuals annually, or are connected with any other key projects deemed appropriate by the Gu's Commissioner will now require the use of big data analysis. The pilot project under the policy is the project for selecting optimal locations for security cameras. The public sector is, thus, accelerating its analyses of big data.[4)]

Despite its importance, the term "big data" itself is interpreted in many ways and as yet lacks a consistent definition. There are two major schools of thought in Korea on the definition of big data. The first defines big data as "an amount of data considered superabundant by present-day managing and analysing capacities."[5)] The second defines big data as "an enormous

---

3) Byungjoo Kim, *KakaoBaengkeuui Iyu Inneun Chogi Heunghaeng Dolpung* [*Why Kakao Bank Has Had Such Great Early Success*], SEDAILY, Sept. 11, 2017, http://www.sedaily.com/NewsView/1OKZI2NCHJ.

4) Seunghoon Kim, *Gangseogu 1-eok Neomneun Jeongchaek Saeop Bikdeiteo Bunseok Sajeonhyeobuije* [*Gangseogu's Pre-Consultation Policy for Big Data Analysis for Projects Exceeding 100 Million Won*], SEOUL PN, Sept. 5, 2017, http://go.seoul.co.kr/news/newsView.php?id=20170906016003&wlog_tag3=naver.

5) Changbeom Lee, *Gaeinjeongbobohobeopje Gwanjeomeseo Bon Bikdeiteoui Hwaryonggwa*

amount of accumulated data and the necessary tools and technologies associated with it."[6] According to Gartner Inc., big data is defined by the three Vs – volume, variety, and velocity – and is characterised by immense quantities (volume); diverse and unconventional forms, such as log history, location information, and multimedia (variety); and, finally, the speed at which it is processed and the rate at which it changes (velocity). The nature of big data necessitates cost-efficient and innovative methods of analysis that allow informed and profitable decision-making.[7]

II. Foreign Legislative Directions (Focusing on Data Privacy Protection Laws)

1. The European Union (EU)

As of 2018, the Data Protection Directive 96/46/EC will be replaced by the General Data Protection Regulation (GDPR) 2016, which is directly enforceable upon European Union (EU) member states. The EU upholds data protection as a fundamental human right, and its legislations demand strict measures for the protection of personal information accordingly.

In particular, Article 4 of the GDPR defines personal information as data relating to an identified or identifiable natural person.[8] This definition is quite similar to that of personal information under the Korean Personal Information Protection Act (PIPA). GDPR also applies to all parties

---

Bohobangnan [*A Study on the Harmonisation of Use of Big Data with Privacy Protection*], 37 BEOBHAKNONCHONG 509 (2013).

6) Hyeyong Yang, *Bikdeiteouirul Whalyonghan Gisulgiwheok Bangbeoplon* [*Methodology of Technology Planning Utilising Big Data*], 2012 KOR. INST. OF SCI. & TECH. EVALUATION AND PLANNING 1, 7–9.

7) *Gartner IT Glossary: Big Data*, GARTNER, http://www.gartner.com/it-glossary/big-data (last visited Oct. 17, 2017).

8) General Data Protection Regulation 2016/679, 2016 O.J. (L119) 1, art. 4 ("'[P]ersonal data' means any information relating to an identified or identifiable natural person ['data subject']; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.").

processing big data (including those operating outside of EU territory) if the processed data include the personal information of an EU individual.[9] Furthermore, the GDPR allows data subjects to request the personal information controller (i) to correct inaccurate information;[10] (ii) to remove unwanted personal information without unreasonable delay;[11] (iii) to block access by third parties and the public to their personal information;[12] and (iv) to refrain from using their personal information for profiling or direct marketing.[13] The data subject may also object to personal data being processed for scientific or historical research and statistical purposes, unless it is necessary for public interest.[14] If the data controller's request is made pursuant to public interest, public authority, or the personal information controller's entitled rights, the data subject may cite the individual's "particular situation" to object to the use of the data subject's personal information.[15]

With regard to pseudonymisation, the GDPR states that pseudonyms should be treated as personal information when they are combinable with other information in a manner that would lead to identification, although the application of information protection obligations to pseudonyms is somewhat more lenient.[16] The GDPR's personal information protection clauses do not apply to anonymous data because these data cannot be used to identify individuals.[17]

The EU Article 29 Working Party (Art. 29 WP) Opinion delivers information and perspectives on various anonymisation techniques, the advantages and disadvantages of each, and their degree of security in an attempt to determine the most appropriate technique for different circumstances.[18] When discussing and analysing anonymisation, the Data

9) *Id.* art. 3.
10) *Id.* art. 16.
11) *Id.* art. 17.
12) *Id.* art. 18.
13) *Id.* art. 21.
14) *Id.*
15) *Id.*
16) *Id.* paras. (26), (28).
17) *Id.* para. (26).
18) *Opinion of the Working Party on Anonymization Techniques*, 05/2014.

Protection Working Party classifies the discussion into two categories: randomisation and generalisation. Then, the Working Party supplements these categories with various topics, including pseudonymisation, differential-privacy, K-anonymity, and L-diversity, among others. Moreover, according to the Working Party Opinion, factors such as the probability of singling out,[19] linkability,[20] and inference[21] are points of vulnerability to consider when assessing the risk of data re-identification.

2. The United States

United States federal law does not include any overarching personal information protection legislation. However, there are approximately thirty (30) notable privacy protection statutes in various fields that apply to both the federal government and private entities. State governments also independently enforce privacy and personal information protection regulations.

The Privacy Act,[22] which is applicable to government sector, defines personal information as data about an individual included in personal records possessed by an administrative body. Such information may include an individual's name, identification number, fingerprints, voiceprints, as well as other linkable data.[23]

The so-called Smart Meter case highlights a potential problem with using big data. Smart Meter is a big data network used by electric companies. Smart Meter reports monthly, hourly, and real-time electricity consumption rates to an electric company, which company then analyses the accumulated big data and calculates in detail the electric consumption

---

19) The probability of identity-exposing personal information being retrieved from a pool of data.

20) The probability of at least two types of information being linked to create possibilities of identity exposure.

21) The probability of identity-exposing personal information being inferred from a set of data.

22) 5 U.S.C. § 552a.

23) Taemin Song, *Ilbonui Bikdeiteo Peuraibeosi Bohobangan* [*Japan's Privacy Protection Measures Regarding Big Data*] 210 KOR. INST. FOR HEALTH AND SOC. AFFAIRS 90 (2014) [hereinafter Song, *Japan's Privacy Protection*].

rates of each household, factory, or region in real-time in order to develop strategies to reduce energy consumption. Indeed, IBM used 1,000 Smart Meters in a municipality comprised of 60,000 residents and reduced electricity consumption by 11 percent. In response to such collection, processing, and utilisation of big data through Smart Meter, many states now require data controllers to acquire opt-in or opt-out consent from consumers to install Smart Meters. A tariff model was also introduced as an option for ensuring privacy protection. The model proposes that consumers be given the right to restrict the Smart Meter's access to their electricity consumption information and that they be charged differently based on whether they provided such access.[24)]

Additionally, the federal Health Insurance Portability and Accountability Act (HIPAA) and the accompanying HIPAA Privacy Rule protect health-related information (*i.e.*, Protected Health Information; PHI). The HIPAA Privacy Rule permits the use and public disclosure of de-identified health-related information without the data subject's consent. Methods proposed[25)] for de-identification in such instances are (i) expert determination[26)] and (ii) safe harbour.[27)] Meanwhile, the Office for Civil Rights (OCR) issued the Guidance on Methods for De-identification of PHI,[28)] which is a more

---

24) Yeongwha Sohn, *Bikdeiteo Sidaeui Gaeinjeongbo Bohobangan* [*A Legal Study on the Protection and Use of Personal Information*], 28(3) Kor. Bus. L. Ass'n 369 (2014).

25) Yoonmi Kim, *Bisikbyeol Jochi Donghyang Mitgungnae Jeogyongeul Wihan Sisajeon Dochul* [*Foreign De-identification Trends and Drawing Implications for Domestic Implementation*], 5 CIS Issue Report 2 (2017) [hereinafter Kim, *Foreign De-identification Trends*].

26) If the risk of identification is determined to be very small by any select individual who is sufficiently knowledgeable and experienced in standard statistical/scientific methods, the data will be considered de-identified.

27) After the eighteen (18) pieces of data listed below are removed and the probability of identification through combining remaining data is null, data will be considered de-identified: 1) name, 2) geographical information in a unit smaller than a state, 3) dates relevant to the individual (birthday, date of death, etc.), 4) phone number, 5) fax number, 6) email address, 7) social security number, 8) medical record number, 9) health insurance beneficiary number, 10) account number, 11) driver's license number, 12) vehicle identifier or serial number (vehicle registration number included), 13) device identifier or serial number, 14) URL, 15) IP address, 16) biometric identifier (fingerprints and voiceprints included), 17) picture of their entire face or similar images, and 18) other serial numbers or codes exclusive to the individual.

28) Guidance Regarding Methods for De-identification of Protected Health Information in Accordance with the HIPAA Privacy Rule.

detailed procedural and evaluative guideline for the aforementioned Expert Determination procedure. "Guidance" requires that a qualified expert determine the risk of identification to be "very small" and that the predicted risks be mitigated by the data manager through statistical or scientific methods of mitigation. The data manager must then consistently re-evaluate the risk of identification and assure that the data's probability of identification upon exposure remains "very small."

3. Japan

Japan's Act on the Protection of Personal Information, which is the primary legislation for personal information protection in that country, defines personal data as "information about a living individual which can identify the specific individual by name, date of birth or other description contained in such information (including such information that can be easily referenced with other information and will thereby enable the identification of the specific individual)."[29] This definition of personal information is also similar to that of the PIPA. Recently, Japan established a concept of "anonymized processed information," a category of information that cannot lead to individual identification.[30] [31] Furthermore, the 2015 amendments to the Act on the Protection of Personal Information added other provisions, such as changes to the purpose of using personal information for which opt-out consent is required, establishment of a private organisation related to the use of personal information, and recognition of the right to disclose personal information.[32]

---

29) Song, *Japan's Privacy Protection*, *supra* note 23.

30) Kim, *Foreign De-identification Trends*, *supra* note 25, at 8.

31) Kojin Jōhō No Hogo Nikansuru Hōritsu [Act on the Protection of Personalized Information], Law No. 57 of 2003 art. 2, para. 9 ("'Anonymized processed information' refers to unidentifiable information obtained from processed personal information. Anonymized personal information cannot be traced back or restored to its original personal information").

32) Sangyook Cha, *Bigdeiteo Hwaryonge Ttareun Gaeinjeongbobohobeopjewaui Chungdolgwa Gwaje* [*Conflicts and Issues Regarding Personal Information Protection Legislation Following the Utilisation of Big Data*], 1 HANYANG UNIV. SCH. OF L. 321 (2016) [hereinafter Cha].

III. On Big Data: Trends in Korea's Policies and Legislations

1. Big Data Promotion Policies and the Dilemma of Data Privacy Regulations

As of August 8, 2017, South Korea's Ministry of Science and ICT (MSIT) announced its plan to invest a total of 6.3 billion Won (approximately USD 6 million), which includes a supplementary budget of 4.3 billion Won (approximately USD 4 million),[33] into artificial intelligence and big data research. Then, on December 8, 2016, the MSIT and the Ministry of the Interior and Safety (MOIS) jointly established a big data task force in cooperation with private parties, and the two ministries have been discussing other systematic measures to stimulate the big data industry. The Korean government is attempting to stimulate the big data industry through such efforts as one of its core missions to prepare for the fourth industrial revolution.

Despite the Korean government's extensive policy efforts to promote the big data industry and the industry's desire to develop big data, past incidents involving big data or personal information[34] have raised strong concerns that the collection, analysis, and circulation of large volumes of data may violate individual privacy rights and liberties, as guaranteed by Article 17 of the Constitution of the Republic of Korea (hereafter, "the Constitution"). Therefore, legislative mechanisms to prevent such

---

33) Hojoon Song, *Ingongjineung AI Bikdeiteo Chasedae Gichoyeongu Jiwoneuro Sacha Saneophyeongmyeonui Gibaneul Teunteunhi Handa* [*Strengthening the Foundation of the Fourth Industrial Revolution through Supporting Fundamental Research of AI and Big Data*], Ministry of Science and ICT, Aug. 8, 2017, http://www.msit.go.kr/web/msipContents/contentsView.do?cateId=mssw311&artId=1358672.

34) For example, Netflix provided movie recommendation services by analysing the movie preferences of individual customers. Following the release of the service, Netflix made 500,000 customer histories public and held a development competition. However, upon examining and cross-referencing data from account histories and internet movie databases, a group from the University of Texas discovered that it was possible to identify each individual data subject in the pattern analysis. Following this discovery, the Federal Trade Commission (FTC) acknowledged problems with privacy and suspended the second competition.

violations may be necessary.

2. Overview of Data Privacy-Related Legislations

The thoroughness of South Korea's data privacy protection regulations essentially rivals that of the EU. As of 2017, the key Korean privacy policy regulations relating to big data are as follows:

- PIPA
- The Act on Promotion of Information and Communications Network Utilisation and Information Protection, etc. ("Network Act")
- The Act on the Use and Protection of Credit Information ("Credit Information Act")
- The Act on the Protection, Use, etc. of Location Information ("Location Data Act")
- The Medical Service Act
- Specialised Credit Financial Business Act
- Electronic Financial Transaction Act
- Act on Consumer Protection in Electronic Commerce

The PIPA is considered the primary statute for privacy protection in Korea, and it applies to both online and off-line service providers. The Network Act applies to all businesses that market and provide services through communications networks for profit.[35] As most businesses use this

35) Jeongbotongshinmang Iyongchokjin Mit Jeongboboho Deunge Gwanhan Beobryul [Act on Promotion of Information and Communications Network Utilisation and Information Protection, Etc.], Act No. 6360, Jan. 16, 2001, *amended by* Act No. 10560, April 5, 2011, art. 2 [hereinafter Network Act].

1. The term "information and communications network" refers to an information and communications system for collecting, processing, storing, searching, transmitting, or receiving information by means of telecommunications facilities and equipment under subparagraph 2 of Article 2 of the Telecommunications Business Act or by utilising computers and applied computer technology along with such telecommunications facilities and equipment;
2. The term "information and communications services" refers to the telecommunications

network to advertise and provide their services, the PIPA and the Network Act are the two most widely applicable legislations in Korea, and they apply to most businesses for that reason. Of course, the general public (or each network user) is also required to comply with the Network Act with regard to the use of a network.

When a specific regulation conflicts with general regulations such as the PIPA and the Network Act, the specific regulation will be given priority in terms of its application. For example, the Credit Information Act, Location Data Act, and Medical Services Act are given priority of application when the involved big data concern credit, locational, and medical information, respectively. The Specialised Credit Financial Business Act and the Electronic Financial Transaction Act are likewise given priority of application to big data regarding the use and application of credit card information and electronic financial transactions, respectively.

In this article, we will focus our discussion on the PIPA and the Network Act, given that both are overarching statutes for privacy regulations. Nevertheless, it should be noted that in most practical applications, general regulations are supplementary to special regulations, and it is necessary to consider both sets of laws for compliance.

3. Definition of Personal Information[36)]

Personal information, as used in Korean legislation, is data that refer to a living individual, such as a full name, a resident registration number,

---

services under subparagraph 6 of Article 2 of the Telecommunications Business Act and services that provide information or intermediate the provision of information by utilising such telecommunications services;

3. The term "providers of information and communications services" refers to the telecommunications business operators included under subparagraph 8 of Article 2 of the Telecommunications Business Act and other persons who provide information or intermediate the provision of information for profit by utilising services rendered by a telecommunications business operator; and

4. The term "users" signifies persons who use information and communications services rendered by providers of information and communications services.

36) Gaeinjeongbo Bohobeob [Personal Information Protection Act], Act No. 10465, Mar. 29, 2011, *amended by* Act No. 14839, July 26, 2017 [hereinafter PIPA], art. 2(1); Network Act, *supra* note 35, art. 2(1)(6).

videos by which an individual can be identified, as well as pieces of information that cannot identify a particular individual on their own but that are easily combinable with other information to lead to identification. According to a ruling by the Seoul Central District Court,[37] personal information is defined as data that, independently or through a simple combination with other information lead to identification of an individual. In this definition, it is not necessary for all relevant and combinable information to be owned by the same person. The term "easily combinable" does not necessarily refer to the ease with which the information can be acquired: rather, it refers to the ease with which this information can be combined with other data to identify the data subject. In sum, enforcement agencies and courts appear to recognise a broad definition of personal information because their definition includes "information that can be combined with other data to identify a person."

As the existing body of laws and regulations in Korea define the concept of personal information so broadly, through the seemingly vague concept of "identifiability," it is naturally difficult to determine what particular information – among immense quantities of information that big data companies manage and process – should be considered personal. Consequently, it is unclear to what extent businesses that employ big data technology are required to comply with the PIPA and other legislations. Such uncertainty limits their production and use of big data.

4. Production of Big Data

1) Self-Owned Data

The production of big data requires basic data. Hence, information that

37) Seoul Central District Court [Dist. Ct.], 2010Go-Dan5343, Feb. 23, 2011 (holding that although International Mobile Equipment Identity [IMEI] or Universal Subscriber Identity Module [USIM] serial numbers themselves are not considered personal information because they are mere combinations assigned to each card, their classification changes from "a serial number assigned to a device or card" to "a serial number assigned to a device or card under the ownership of a specific individual" once they are delegated to customers; holding also that there are grounds to consider them personal information because carrier application forms and other application information can be easily traceable from IMEI and USIM serial numbers).

has already been collected is the starting point for producing big data.

2) Third-Party Data

In addition to self-collected data, businesses often acquire data from third-party providers. Many businesses also acquire data from their affiliates. Because many Korean companies operate under a conglomerate structure (*i.e.*, *Chaebol* in Korean), it is already (or soon will be) customary practice for Chaebol entities to collect, process, and analyse all data from various affiliates and share such data with other affiliates. Such structures are not unique to the South Korean Chaebol system; many foreign international companies appear to be doing the same.

Businesses also give data to third parties through cooperative arrangements. For instance, credit card companies use subscriber information to run joint marketing campaigns with insurance companies. In the case of annually renewable automotive insurance, credit card companies and insurance companies often have cooperative arrangements in which the insurance company gives the credit card company information on which subscribers' insurance coverages are due to expire; in turn, the recipient credit card company is allowed to market their services to such subscribers jointly with the insurance company. An obvious prerequisite to such marketing practices is the consent of each credit card subscriber, who is also an insurance holder.

3) Publicly Available Data

Businesses can also create big data from publicly available data. For instance, information made available on the websites of schools, companies, or other entities may be collected and commercialised. However, such practices raise privacy concerns as well. Some argue that an individual's consent to have their information made public on a website does not extend to the collection and unlimited commercialisation of the same information. We note a Korean Supreme Court case that highlights this issue. In this case, a company collected personal information about professors from law school websites and used it for commercial purposes. This is one of the company's business activities. In this case, the Korean Supreme Court decided that the defendant company did not violate the data privacy laws because the relevant personal information was already disclosed to the

public, and the purpose of the defendant company is similar to that of the public disclosure. In this case, the defendant company's business is to introduce law-related information, including statutes, court cases, and information of law professionals, including professors, lawyers, judges and prosecutors.[38)]

4) Data Acquisition Transaction

Businesses also often collect data through mergers, acquisitions, as well as transfer, sale, or assignment of businesses or assets. In such cases, privacy regulations apply in addition to other laws and regulations. The PIPA and Network Act also acknowledge special clauses for this instance, as discussed below.

5. Opt-In Principle

Informational self-determination rights grant individuals the right to determine when and to what extent their personal information may be collected and with whom it may be shared. It is the data subject's right to determine the disclosure and use of their personal information.[39)] The constitutional grounds for informational self-determination are derived from Article 17 of the Constitution, which guarantees the right to privacy, and Article 10, which guarantees the rights to human dignity and the pursuit of happiness. To protect the rights conferred by informational self-determination, Korean regulations require, in principle, opt-in consents by data subjects before their information may be collected, used, or provided to a third party.

It appears that most businesses in Korea acquire their data subjects' consents when using personal information for big data or marketing. However, complications may arise when subscribers of businesses that have been in operation for many years – who provided prior consents – have not yet consented to the utilisation of their personal information for the specific purpose of big data utilisation and marketing purposes. In such cases, the business needs to amend its personal information management

38) Supreme Court [S. Ct.], 2014Da235080, Aug. 17, 2016.

39) Supreme Court [S. Ct.], 99Hun-Ma513, May 26, 2005.

policy and concurrently acquire consent to the same pursuant to Article 17 of the PIPA's enforcement decree[40] and Article 12 of the Network Act's enforcement decree.[41] Without such consent, creating big data from

---

40) Gaeinjeongbo Bohobeob Sihaengryung [Enforcement Decree of the Personal Information Protection Act], Presidential Decree No. 28355, Oct. 17, 2017, art. 17.

(1) A personal information controller shall obtain consent from a data subject to the processing of his/her personal information pursuant to Article 22 of the Act by any of the following methods:

1. To issue a document stating the matters requiring consent, either in person or by mail or facsimile, to the data subject, and obtain a written consent on which the data subject has affixed his/her signature or seal;
2. To inform the data subject of the matters requiring consent, and confirm his/her intent of consent by telephone;
3. To inform the data subject of the matters requiring consent by telephone, let him/her to confirm the matters requiring his/her consent posted on the designated website, etc.; and reconfirm his/her intent of consent by telephone;
4. To post the matters requiring consent on the designated website, etc., and let the data subject to express his/her consent to it;
5. To send an electronic mail containing the matters requiring consent to the data subject, and receive the return e-mail with his/her consent to it; [and]
6. Other methods to inform the data subject of the matters requiring consent by a method similar to those referred to in subparagraphs 1 through 5, and confirm his/her intent of consent.

41) Jeongbotongshinmang Iyongchokjin Mit Jeongboboho Deunge Gwanhan Beobryul Sihaengryung [Enforcement Decree on the Act on Promotion of Information and Communications Network Utilisation and Information Protection, Etc.], Presidential Decree No. 23169, Sept. 29, 2011, *amended by* Presidential Decree No. 23876, June 25, 2012, art. 12.

(1) Pursuant to Article 26-2 of the Act, a provider of information and communications services shall obtain consent by any of the following methods: In such cases, a provider of information and communications services shall state matters for which he/she shall obtain consent (hereinafter referred to as "matters subject to consent") so that users can clearly recognise and check such matters: <Amended by Presidential Decree No. 21278, Jan. 28, 2009>

1. Publishing matters subject to consent on his/her website and requesting each user to express whether he/she consents thereto;
2. Delivering a document containing matters subject to consent to each user in person or by mail or facsimile and requesting the user to return the document with his/her signature or seal affixed, if he/she consents thereto;
3. Sending a document containing matters subject to consent to each user by e-mail and requesting the user to return it with his/her consent expressed thereon by e-mail; [and]
4. Informing each user of matters subject to consent by telephone and obtaining consent from the user or informing each user of a method by which the user can check the

information that contains personal information about past subscribers will be difficult.

According to the PIPA and the Network Act, if opt-in consent is not acquired, then the following liabilities may arise:

> (1) Criminal prosecution: the subjected business (corporation) and the individual violator may face up to five years in prison or be fined a sum of up to 50 million Won.[42] Furthermore, any monetary amount or other profit acquired through the violation may be subject to confiscation; if confiscation is impracticable, the violator may be fined an amount commensurate with such profit;[43]
> (2) Administrative sanctions: the subjected business (corporation) may also be liable to pay a penalty of up to three percent of sales revenues related to the violation.[44] Furthermore, if the violator is an information and communications service provider, the Korea Communications Commission (KCC) and/or Minister of the MOIS may recommend (*de facto* order) the violator to take disciplinary action against the violator (including its representative and responsible executive officers). The violator shall respect the recommendation and report to the agency on the result of such disciplinary actions;[45] and
> (3) Civil liability: violators may be civilly liable to data subjects. In Korea, the burden of proof has transitioned,[46] so now the violator

---

relevant Internet address and matters subject to consent and then calling the user again to obtain consent over the telephone.

(2) If it is impracticable for a provider of information and communications services to fully state matters subject to consent due to the characteristics of the medium for collecting personal information, he/she may inform each user of a method by which the user can check matters subject to consent (Internet address, telephone numbers of the place of business, etc.) to obtain consent from the user. <Amended by Presidential Decree No. 21278, Jan. 28, 2009>

42) PIPA, *supra* note 36, art. 71(1)(2); Network Act, *supra* note 35, art. 71(1)(3).

43) PIPA, *supra* note 36, art. 75-2.

44) Network Act, *supra* note 35, art. 64-3(1)(3).

45) PIPA, *supra* note 36, 65(3); Network Act, *supra* note 35, art. 69-2(2).

46) PIPA, *supra* note 36, art. 39(1); Network Act, *supra* note 35, art. 32(1).

must prove that it was not intentional or negligent in causing harm; otherwise must compensate data subjects for damages suffered.[47] Such compensation may be up to triple the damages as a form of punitive damages.[48] Statutory damages regulations may also apply.[49]

---

47) Regulations regarding punitive or statutory damage reimbursements have only been in force as of July 2016. Therefore, cases wherein they have been applied do not yet exist. With regard to the case referenced in footnote 50 (an incident wherein personal information was provided to a third party without the consent of the data subjects), the Suwon District Court ruled in favour of the civil liability charges brought forward by the plaintiffs and declared that Homeplus (a supermarket chain) must pay a fine of 50,000 or 150,000 Won to 425 plaintiffs. With regard to personal information leakage cases, the following applies: (i) In the so-called e-Bay Auction case, the Supreme Court ([S. Ct.], 2013Da43994, Feb. 12, 2015) ruled that in an instance wherein the information and communications service provider has fulfilled both technical and managerial protection requirements in adherence to the Network Act and its enforcement decree and has followed the "criteria for the technical and managerial measures for the protection of personal information" as outlined by the Ministry of Information and Communication, it is difficult to accuse them of violating any legal or contractual terms for the protection of personal information. (ii) In instances wherein it is difficult to establish whether the data controller has fulfilled its legal and contractual obligations to protect personal information, the Seoul Central District Court ([Dist. Ct.], 2012Ga-Hab81628, Aug. 22, 2014) declared that the defendant (KT, a telecommunication company) pay each plaintiff 100,000 Won (approximately USD 90) per plaintiff; the case was appealed and is currently pending at Seoul High Court. Another similar judgement was rendered in connection with the data breach case that occurred in January of 2014, in which more than 100 million customers' personal data were exposed by three credit card companies. Under the court ruling, the three credit card companies involved were ordered to pay 100,000 Won (approximately USD 90) to each plaintiff.

48) PIPA, *supra* note 36, art. 39(3) ("Where a data subject suffers damage out of loss, theft, divulgence, forgery, alteration, or damage of his/her own personal information, caused by wrongful intent or negligence of a personal information controller, the Court may determine the damages not exceeding three times such damage, provided that the same shall not apply to the personal information controller who has proved non-existence of his/her wrongful intent or negligence."); Network Act, *supra* note 35, art. 32(2) ("Where any damage occurs to a user because personal information has been lost, stolen, leaked, forged, altered, or damaged due to intention or gross negligence on the part of the provider, etc. of information and communications services or similar, a court may determine the amount of compensation to the extent not exceeding three times the said damage: Provided, That this shall not apply where the provider, etc. of information and communications services proves that there is neither intention nor gross negligence on the part of the said provider.").

49) PIPA, *supra* note 36, art. 39-2:

(1) Notwithstanding Article 39 (1), a data subject, who suffers damage out of loss, theft, divulgence, forgery, alteration, or damage of his/her own personal information, caused

As of July 1, 2016, the Korean government announced the "Guidelines for De-identification of Personal Data" (hereafter the "De-identification Guidelines"), which declares that de-identified personal data is no longer "personal information" and permits a relatively unconstrained use of de-identified data without acquiring the data subject's consent. The announcement of such guidelines can be understood as a countermeasure against the complaint that privacy laws excessively restrict the production and use of big data. However, this change in policy faces strong opposition because there have been widely reported incidents of data breach in Korea. For example, Homeplus (a supermarket chain) was indicted for collecting twenty four (24) million pieces of personal information and selling each for

---

by wrongful intent or negligence of a personal information controller, may claim a reasonable amount of damages not exceeding three million Won. In this case, the said personal information controller may not be released from the responsibility for compensation if it fails to prove non-existence of his/her wrongful intent or negligence.
(2) In the case of a claim made under paragraph (1), the court may determine a reasonable amount of damages not exceeding the amount provided for in paragraph (1) taking into account all arguments in the proceedings and the results of examining evidence.
(3) A data subject who has claimed compensation pursuant to Article 39 may change such claim to the claim provided for in paragraph (1) until the closing of fact-finding proceedings.

See also Network Act, *supra* note 35, art. 32-2:

(1) Where a user falls under each of the following subparagraphs, he/she may claim reasonable compensation not exceeding three million Won as damages, in lieu of claiming damages under Article 32 from a provider of information and communications services, etc. within a period prescribed by Presidential Decree. In such cases, the relevant provider of information and communications services, etc. cannot be exempt from responsibility unless he/she proves that there is no intention or negligence: <Amended by Act No. 14080, Mar. 22, 2016>

1. Where the provider of information and communications services, etc. violates any of the provisions of this Chapter by intention or negligence;
2. Where personal information is lost, stolen, leaked, forged, altered or damaged.

(2) Where a claim for compensation under paragraph (1) is filed, a court may acknowledge a reasonable amount of loss within the limits prescribed in paragraph (1), taking into account the relevance of all pleadings and the outcomes of examination of evidence.

(3) A user claiming compensation for damage pursuant to Article 32 may change such claim to the claim referred to in paragraph (1) before the argument of the inquisition is closed. <Newly Inserted by Act No. 14080, Mar. 22, 2016>.

2,800 Won to an insurance company to accrue profits of 23.1 billion Won.[50] Also, an international big data company, IMS health, covertly purchased 44 million pieces of Korean citizens' personal information from hospitals and pharmacies and sold them to a pharmaceutical company to turn a profit of seven billion Won. Such cases bolster the position of critics, who argue that the De-identification Guidelines only serve the interests of the big data industry and that the right to informational self-determination would practically be non-existent if de-identified data – which can easily lead to identification if cross-referenced with other information – can be utilised without consent.[51]

In a recent case, Google email service users in Korea cited the Network Act[52] to demand that the defendants, Google Korea Ltd. and Google, Inc.,

---

50) Suwon District Court [Dist. Ct] 2015Ga-Hap1847, Aug. 31, 2017.

51) Sukjin Yoon, *(Bisikbyeoljeongbo Hwaryong Nollan) (1) Jeongbu "Bikdeiteo Hwalseongwha" vs. Simindanche "Gaeinjeongbo Chimhae" [(The Issue that Arises from the Utilisation of Big Data) (1) Government "Vitalising the Use of Big Data" vs. Civic Group "Violation of Privacy"]*, NEWS TOMATO, July 12, 2016, HTTP://WWW.NEWSTOMATO.COM/READNEWS.ASPX?NO=671708.

52) Network Act, *supra* note 35, art. 30(2)(2):

> (1) Every user may, at any time, revoke his/her consent given to a provider of information and communications services or similar to allow the provider to collect, use, or furnish his/her personal information.
>
> (2) Every user may request a provider of information and communications services or similar to allow him/her to peruse, or to furnish with any of the following subparagraphs, and may also require the provider to correct an error, if there is any error:
>
> 1. Personal information of the user, which the provider of information and communications services or similar possesses;
> 2. Details for which the provider of information and communications services or similar has used personal information of the user or furnished it to a third party; [and]
> 3. Details for which the user has given a consent to the provider of information and communications services or similar to collect, use, or furnish his/her personal information.
>
> (3) If a user withdraws his/her consent pursuant to paragraph (1), a provider of information and communications services, etc. shall immediately take necessary measures, such as the destruction of collected personal information in an irrecoverable or in unreproducible way. <Amended by Act No. 12681, May 28, 2014>
>
> (4) A provider of information and communications services or similar shall, in receipt of a request to peruse or furnish matters in accordance with paragraph (2), take necessary measures without delay.

disclose to the plaintiffs which personal information was provided to third parties (and other related details). Seoul High Court held that the definition of "personal information" in Article 2(1)(6)[53] of the Network Act includes not only information that directly identifies individuals, but also information that can be easily combined with other data to lead to identification. Ultimately, the Court held that because the de-identified information met the above definition, the de-identified information was personal information.[54] Based on this finding, the Court held that Google had an obligation to disclose the details on the provision of personal information to third parties, as listed in Appendix 2 of the plaintiffs' exhibit. Notably, the Court's holding that the de-identified information (*i.e.*, anonymous identifiers that identify a user once and are later disposed of) described in Appendix 2 (a. 8)[55] of the plaintiffs' exhibit constituted

---

(5) A provider of information and communications services or similar shall, in receipt of a request for correction of an error in accordance with paragraph (2), correct the error, notify the user of the reasons why it is unable to correct the error, if it is the case, or take any other necessary measures, and may not use the relevant personal information or furnish it to a third party until he/she completes taking such measures, provided that he/she may furnish the personal information to a third party or use the information, if requested to furnish the personal information pursuant to any other Act.

(6) A provider of information and communications services or similar shall make how to revoke consent under paragraph (1), how to request to peruse personal information or furnish such information under paragraph (2), and how to request correction of an error easier than how to collect personal information.

(7) Paragraphs (1) through (6) shall apply mutatis mutandis to a transferee of business or similar. In such cases, "provider of information and communications services or similar" shall be deemed "transferee of business or similar."

53) Network Act, *supra* note 35, art. 2(1)(6).

54) Seoul High Courts [Seoul High Ct.], 2015Na2065729, July 26, 2017, appeal docketed, No. 2017Da219232 (Kor. S. Ct.) filed by the defendants and plaintiffs.

55) **Appendix 2. Areas of information and history of service usage provision statuses subject to disclosure obligations**

a. In accordance with Article 2 (1) of the PIPA and Article 2 (1) 6 of the Network Act:

(1)~(7): omitted

(8) Cookies or data of visited web pages, data saved through add-on features, download histories on websites, cookies that can uniquely identify a user's browser or Google account, cookies that can be collected/stored when Google features or advertisement services offered to partners (publishers, advertisers, or connected websites) interact with users, cookies collected and stored by Google Analytics, information Google received from partners which was connected to users' Google accounts, information

personal information may actually conflict with the De-identification Guidelines.

In the era of big data, information that cannot independently identify a particular individual still holds the potential to become personal information which could identify a particular individual during the course of analysis through big data technology. For example, Amazon.com systematically collects and analyses individual customers' purchase histories to tailor product recommendations to each customer. Information collected while analysing an individual customer's data may be deemed secondary (derived) data, and Amazon.com processes such data without obtaining the consent of the data subjects. If the individual customer does not explicitly consent to the use of secondary information, the question remains whether using such data should be considered a violation of Korea's privacy laws.

The authors maintain that data subjects' *general* consent to collection and use of their personal information ought to be sufficient for the data processor to use secondary data without acquiring further consent. As technological advances continue to broaden the scope of how primary information may be used, it is virtually impossible to acquire opt-in consents in anticipation of the future. It is impracticable to require businesses to acquire a new consent each time a new need arises. Hence, the interpretation that "any use of secondary information without additional consent violates privacy laws" excessively hampers development of the big data industry.

On another note, the De-identification Guidelines require businesses to monitor any likelihood of the re-identification of de-identified information and, if this is the case, to (i) cease processing such re-identified information; (ii) implement procedures to protect such information; (iii) destroy any re-identified information immediately; and, (iv) de-identify this information again before use. Given that such procedures are quite thorough and

---

Google collects when users are logged in, [and] all such information classified (*i.e.*, "interest settings," "security," "process," "advertisement," "session status," and "web-log analysis") and collected by Google as cookies or **anonymous identifiers (a disposable identifier that can identify a user once)**.

b. Content of emails, dates of transmittance and reception, names and email addresses of senders and recipients, and other information pertaining to the use of Gmail services.

extensive, they appear to be a sufficient compromise between data privacy and use.[56)]

6. Third-Party Provisions (Sharing Personal Information with a Third Party)

Parties are required to attain explicit consent before providing personal information to third parties.[57)] [58)] When acquiring consent, the third party

---

56) Cha, *supra* note 32, at 337 (explaining that there are conflicting perspectives regarding the guidelines' allowance of re-identified data to be de-identified and re-employed; one view is that allowing the usage of re-identified data by a re-de-identifying process may violate PIPA regulations).

57) PIPA, *supra* note 36, art. 17:

(1) The personal information processor may provide (or share, hereinafter the same applies) the personal information of data subjects to a third party in the case applicable to any of the following Subparagraphs:

1. Where the consent is obtained from data subjects; or
2. Where personal information is provided within the scope of purposes for which personal information is collected under Subparagraphs 2, 3 and 5 of Article 15(1);

(2) The personal information processor shall inform data subjects of the following when it obtains the consent under Subparagraph 1 of Paragraph (1). The same shall apply when any of the following is modified:

1. The recipient of personal information;
2. The purpose of use of personal information of the said recipient;
3. Particulars of personal information to be provided;
4. The period when personal information is retained and used by the said recipient; and
5. The fact [about] which data subjects are entitled to deny consent, and disadvantage affected resultantly from the denial of consent. (3) When the personal information processor provides personal information to a third party overseas, it shall inform data subjects of any Subparagraphs of Paragraph (2), and obtain consent from the data subjects. The personal information processor shall not enter into a contract for the cross-border transfer of personal information in violation of this Act.

58) Network Act, *supra* note 35, art. 24-2:

(1) Every provider of information and communications services shall, whenever he/she intends to furnish a third party with personal information of a user, notify the user of all the following matters and obtain consent from the user, except as provided for in Article 22 (2) 2 and 3. The same shall apply in cases where there is a change in any of the

must be identified explicitly: it is not permitted to expand the scope of third parties by using "etc." or similar language. Hence, whenever additional third parties need to be added, additional consents are necessary.

Affiliates, as well as parents and wholly-owned subsidiaries of a party, are also considered third parties. Some foreign companies do not specifically list company names on consent forms and instead write "subsidiary of *** company." Some argue that this level of specificity is sufficient and should be considered legal because such descriptions afford data subjects reasonable foreseeability. In practice, however, courts and regulatory authorities consider such descriptions to be illegal.

As further elaborated upon below, providing personal information to third parties is not the same as the *entrustment* of personal information to third parties. If, on the one hand, personal information is given for the benefit of the receiving party, such provision is classified as third party provision of personal information. If, on the other hand, personal information is entrusted to a third party to be processed for the benefit of the providing party, such provision is classified as the entrustment of personal information. For instance, if a credit card company uses the

---

following matters:

1. The person to whom the personal information is furnished;
2. Purposes of use of the personal information of the person to whom the personal information is furnished;
3. Items of the personal information furnished; [and]
4. Period of time during which the person to whom the personal information is furnished will possess and use the personal information.

(2) A person who received any personal information of a user from a provider of information and communications services in accordance with paragraph (1) shall not furnish the personal information to a third party or use it for any purpose other than the purpose originally agreed upon at the time when the information was furnished without consent of the user or a specific provision otherwise specified in any other Act.

(3) When the provider, etc. of information and communications services under Article 25 (1) is given consent to furnishing the user's information under paragraph (1) and to the entrustment of management of personal information under Article 25 (1), he/she shall obtain such consent apart from the consent to collection/use of personal information pursuant to Article 22, and shall not refuse to provide its service on the ground of a user's refusal of aforementioned consent.
<Newly Inserted by Act No. 10560, Apr. 5, 2011; Act No. 14080, Mar. 22, 2016>.

services of a third party to deliver credit card invoices to consumers, the provision of personal information to that third party would be considered entrustment. For personal information entrustment, a notice of entrustment to the data subject is sufficient, and explicit consent is not required as long as such entrustment is essential to the performance of contract between the business and the data subject (otherwise, a consent from and/or separate notice must be given to the data subject). In practice, however, the line between entrustment and third-party provisions is often nebulous. In a recent ruling by the Supreme Court of Korea, parties who regarded their information transaction as a form of entrustment and entered into a contract with a third party without having acquired third-party provision consents were found liable for violating privacy rights.[59)]

7. Privacy Law Restrictions: Difficulties Regarding Cross-Border Transfers

Many multinational corporations collect personal information from subsidiaries in Korea, have this information transferred overseas to be compiled as big data, and then have it analysed in their respective territory. According to Article 17(2) of the PIPA, when personal information is transferred to a third party abroad, consent to the following is required:

1. The recipient of personal information;

---

59) Supreme Court [S. Ct.], 2016Do13263, April 7, 2017 (holding that with regard to the entrustment of personal information and third-party personal information provisions, although 'third-party provisions of personal information' as stated by art. 17 of the PIPA and art. 24-2 of the Network Act are transactions of data that extend beyond explicitly stated purposes of collection and use of personal information for the operational and financial benefit of the receiving party, art. 26 of the PIPA and art. 25 of the Network Act refer to processing entrustments of personal information as data transactions that adhere to the originally stated purposes of collection and use of personal information that serve to benefit the operation or profit of the providing party; holding also that the determination of whether or not a practice is a provision of personal information or a processing entrustment of personal information should take into consideration the purpose and method used for the collection of personal information, status of fee-provision, status of the transferor's supervision of the fiduciary, effects regarding personal information protection requirements on data subjects by such data transactions, and whether the use of respective personal information is truly necessary based on who the beneficiaries of this information will be).

2. The purpose of use of personal information by the recipient;
3. Details on the personal information that is provided;
4. The period during which personal information will be retained and used by the recipient; and
5. The fact that data subjects are entitled to withhold consent and the disadvantage(s) of withholding consent, if any.

Additionally, according to Article 63(2) and (3) of the Network Act, the data subject's consent is required even in instances where personal information is transferred for the sole purpose of being stored in the business' own servers overseas. However, no consent is necessary if (i) the transfer is necessary to promote user convenience, (ii) the personal data controller complies with contractual obligations related to the provision of information communication services, and (iii) the personal data controller informs the data subject of all the following:

1. Which personal information is being transferred;
2. The country to which the personal information will be transferred, the date and time of transfer, and the method of transfer;
3. The name of the personal information recipient (if the recipient is a legal entity, the name of the entity and the contact information of the person responsible for managing the information);
4. The purposes of use of the personal information recipient, and the duration of retention and use of the personal information.

8. Outsourcing the Processing of Data

Numerous corporations employ professional big data processors, which is a form of entrustment of personal information. According to Article 26(2) of the PIPA and Article 28(2) of the Enforcement Decree of the PIPA, the entrustment of personal information in this type of situation does not require consent: the transferor only needs to disclose the identity of the transferee on the transferor's website. In such instances, however, the transferor must enter into an agreement with the transferee, which should cover matters required by Article 26(1) of the PIPA and Article 28(1) of the Enforcement Decree of the PIPA (*i.e.*, the purpose and scope of outsourced

work; limitations to re-outsourcing; measures to ensure safety, including restricting access to personal information; and supervising the status of the management of personal information that is retained in relation to outsourcing). Furthermore, pursuant to Article 26(6) of the PIPA, if the transferee violates the PIPA, then the transferee is considered an employee of the transferor for the purposes of determining liability.

When communication network service providers entrust their users' personal information to a third party, the application of the Network Act is given priority. According to Article 25 of the Network Act, the data controller is required to notify the data subject of the identity of the transferee and the tasks with which they are entrusted, subsequently acquiring the data subject's consent. However, if entrustment is necessary to perform a contract on communications network services and to promote user convenience, it is sufficient to deliver notice to the data subject rather than obtain their consent.

A contract on communications network services likely does not include processing and using big data owned by the company for marketing purposes. In such instances, therefore, data controllers need to acquire separate consents from data subjects.

9. Use of Publicly Available Data

As discussed above in regard to using publicly available data to generate profit, the Korean Supreme Court held that the defendant's (business's) publication of personal information for profit without acquiring consent was not a violation of the PIPA for three reasons. First, the personal information was readily available to the general public through an accessible platform (on the website of the university's law department, there was a list of professors and professors' information). Second, the defendant published the information as it was. Third, the applicable information was public in nature.[60] The Supreme Court elaborated on the meaning of Article 20 of the PIPA by holding that when collecting and processing personal information already publicly available, a

60) Supreme Court [S. Ct.], 2014Da235080, Aug. 17, 2016.

data controller is required—upon a data subject's request—to disclose three things to the data subject. First, the source of the collected personal information. Second, the purpose for processing the personal information. Third, the fact that the data subject may demand that the processing of the personal information be suspended, pursuant to Article 37 of the PIPA.[61] The Supreme Court held that such *ex-post-facto* remedies preserve the data subject's right to informational self-determination.

However, in the above case, the defendant was a website that provided legal information for a fee, and the plaintiff (data subject) was a law-school professor. The Court held as it did based on the public nature of the personal information, such as students' right to know their professors. Therefore, this decision should not be considered an overarching norm. Instead, a thorough analysis of liability should consider various factors, such as the nature of published personal information and the nature of business that processes and publishes such information, among others.

10. Mergers and Acquisitions, Data Transfer, and Integration

Parties often undergo mergers or acquisitions to transfer or acquire data needed to compile big data. A corporation may transfer personal information to a third party by partially or entirely assigning or merging its business operations. In such a situation, a data controller is required to only notify the data subjects that the transfer of personal information is underway and of the identity of the transferee. Additionally, the data controller is required to notify those who oppose the transfer of possible remedies and the procedures for seeking them. Disclosing such information on the data controller's website for at least 30 days is sufficient if the data subjects are difficult to reach.[62] The transferee of the data, in such a case, may use only the personal information in the data in accordance with the originally stated purpose of use. Article 26 of the Network Act and Article 32 of the Credit Information Act contain similar provisions. However, a financial institution transferring additional credit information requires approval by the Financial Services Commission.

---

61) *Id*.

62) PIPA, *supra* note 36, art. 27.

11. Marketing Restrictions on Big-Data Analyses

A key purpose of processing big data is to improve business marketing. Article 50 of the Network Act and Article 51 of the Enforcement Decree of the same requires explicit opt-in consent from each respective recipient (target consumer) before transmitting marketable data to the recipient through electronic transmission media for profit.[63] However, for the first six months after the termination of a business relationship regarding a particular type of commodity, sending marketable for-profit data concerning commodities of the same type is permissible.

12. Big-Data Guidelines (the De-identification Guidelines)

The de-identification guidelines aim to abate privacy-regulation strictures that restrict the growth of the big-data industry. According to the guidelines, de-identified information is no longer considered personal information; the guidelines thereby partially and indirectly relax privacy regulations. The de-identification guidelines comprise the following four steps for the de-identification of personal information.

1. Review—assess whether the information constitutes personal data.
2. De-identify—remove or replace personal-information identifiers from aggregate data in order to render the information insufficient to identify individuals.
3. Evaluate appropriateness—evaluate the de-identification status using an evaluating committee. The committee should include a legal professional and a professional in the de-identification process from a pool of experts recommended by respective professional institutions (*e.g.*, the Korea Internet and Security Agency).
4. Follow up—monitor and prevent the re-identification of the de-identified data.

63) Additionally, the term "marketable data" includes information with marketing content, even if the primary purpose of the information is not marketing.

When data owned by different businesses are combined, identifiers designated for particular individuals may function as matching keys that can identify individuals, so alternative temporary keys can be necessary matching keys that prevent re-identification. Professional institutions oversee the combination of data by using such alternative temporary keys in such instances. Businesses are prohibited from sharing information and algorithms regarding the production of alternative temporary keys, and professional institutions are required to delete alternative temporary keys upon the completion of databases and to give combined databases to businesses with alternative temporary keys removed. Following such a database handover, each business is required to evaluate appropriateness again, as explained above.

IV. Legislative Changes in the Big-Data Industry

This paper has explored laws and regulations related to the big-data industry in South Korea and other jurisdictions. The following are various regulatory changes under discussion.

1. Transition to Opt-out Consents

In order to stimulate the big-data industry, some scholars proposed that opt-in consents should be opt-out consents. The rationale behind the proposal is that in view of the vast amounts of data and the large number of data subjects in the industry, acquiring opt-in consents for every case is not feasible if not impossible. It is not always clear at what stage personal-information controllers must fulfil consent requirements because risk of identification may arise during de-identified data processing. However, opponents of this change are concerned that opt-out consents may violate constitutional rights that guarantee informational self-determination.

2. Restricting the Definition of Personal Information

Some scholars argued that the current definition of personal information stunts the growth of the big-data industry. The definition,

according to laws such as the PIPA, includes information that can be combined with other information to identify individuals. Those who strongly emphasise the importance of privacy protection argue that it is crucial that combinable or linkable information be categorised as personal information. As the PIPA's definition of personal information is similar to its definitions in the EU and Japan, it is difficult to claim that South Korea's broad definition of "personal information" is exceptional. Outside of Korea, there is no dialogue concerning restricting the definition of personal information for the purpose of stimulating the big-data industry.[64]

3. Different Perspectives: Privacy versus Big Data

Legislative changes aimed at stimulating the big-data industry must consider not only the constitutional right to privacy but also the many advantages big-data technology confers on individuals as consumers in the medical, tourism, shopping, and educational-services industries. Another perspective that must be considered is that the utilisation of big data is merely the practice of property rights—property owned by the respective companies. The prevailing perspective in the United States is to prioritise innovation, so the use of big data is deemed favourable. The prevailing thought in the EU, however, is that privacy rights are fundamental human rights. In the United States, informational privacy right is deemed a type of property right, so the right to information privacy is secondary to fundamental constitutional rights, such as the right to know or the right to freedom of expression.[65] Consequently, rights such as the EU's right to be forgotten, with which a data subject may request that internet service providers remove or correct personal information, are not recognised in United States statutes in general.[66]

The different legislative approaches of the EU and the United States likely stem from the different cultures, histories, and values held by the

---

64) Cha, *supra* note 32, at 203.

65) Junghoon Park, "*Eityeojil Gwolliwa Pyohyeonui Jayu, Geurigo Jeongbopeuraibeosi*" ["*The Right to be Forgotten, Freedom of Expression, and Informational Privacy*"], 14(2) KOR. COMPARATIVE PUB. L. ASS'N 594 (2013).

66) Cha, *supra* note 32, at 225.

constituent members of the societies. In a manner similar to the EU, South Korea enforces strict regulations concerning the protection of personal information. The strict tone of South Korea's legislative direction was, and continues to be, reinforced by data-breach incidents, such as the data-breach scandal of 2014 in which 100 million pieces of personal credit information from three credit-card companies were leaked. Such personal information-breach cases intensified public concerns about privacy protection. Moreover, defamation, harassment, and privacy breaches that routinely occur on the internet deepen South Korean fears regarding the exposure of personal information on the internet.

V. Conclusions and Recommendations

Considering the above factors, legislative changes involving one-sided concessions of individual privacy will likely be met with public resistance. However, neglecting legislations that hamper the growth of the big-data industry will undoubtedly cast Korea from the fourth Industrial Revolution. Hence, it is necessary to explore comprehensive measures to reconcile the two perspectives. As a matter of priority, big-data analysis should be divided into two types of analysis based on purpose (*i.e.*, learning about a particular individual [the former] and analysing or predicting social phenomena, namely, making decisions or predicting the future [the latter]). It would be reasonable to continue requiring opt-in consents when individuals are profiled or when data is analysed, such as during marketing-strategy developments that analyse individual consumption patterns, when big-data analysis is meant to be traced back to a particular data subject (the former). However, it would also be reasonable to exempt opt-in consent requirements if such profiling or data analyses were used for demand predictions, decisions concerning companies' business strategies, or statistical analyses in which information will not be used to identify data subjects (the latter). Even in the latter, for cases in which re-identification becomes likely, it would be necessary to notify data subjects and acquire *ex-post* consents. Operating under the above principles, it would be sensible to relax requirements for businesses (*e.g.*, by allowing businesses to replace *ex-ante* consents with *ex-post* consents) that promote

public interests, such as medicine, education, and science, if they meet specific government criteria. It would be important, however, to sanction data processors that abuse big-data technologies or neglect related obligations.