BRUSSELS PRIVACY HUB
WORKING PAPER
VOL. 2 • N° 7 • OCTOBER 2016

BRUSSELS PRIVACY HUB
Vrije Universiteit Brussel

STRUCTURE AND ENFORCEMENT OF DATA PRIVACY LAW IN SOUTH KOREA

by Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung[1]

Abstract

South Korea's data privacy law has evolved rapidly, in particular during the past several years, despite a short history of relevant legislation and enforcement. South Korea's data privacy law has exceedingly stringent consent requirements. In addition to consent, there are many other statutory provisions with onerous requirements, arguably making the overall data privacy law regime in South Korea one of the strictest in the world. South Korea's data privacy law, in particular the Personal Information Protection Act (the PIPA), has a similar structure to the EU's data privacy law. However, the overall legal regime for data privacy and also its enforcement mechanism reveal South Korea's unique characteristics and its weaknesses. In terms of the overall legal regime for data privacy, one interesting characteristic is that, in addition to the PIPA, an omnibus data privacy statute, there are multiple additional statutes governing data privacy issues for specific sectors or industries. In terms of the enforcement of data privacy law, a multitude of government agencies and institutions are in charge. Thus, depending on applicable statutes and other factors, different agencies or institutions could be in charge. Issues on data privacy has gained notable traction in recent years in South Korea and, perhaps reflecting this phenomenon, relevant laws and regulations have been amended frequently. A notable trend is to strengthen penalty provisions and, in particular, the maximum amount of administrative fine is now set at 3% of relevant sales revenue. It remains to be seen if heightened penalty provisions will indeed help addressing data privacy concerns in a meaningful manner.

Keywords: Data privacy, South Korea's data privacy law, Personal Information Protection Act

Contents

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. Available at www.brusselsprivacyhub.org/publications.html ISSN N° 2565-9979. This version is for academic use only.

1. Introduction

South Korea is an IT powerhouse in Asia noted for its technology companies and ubiquitous high-speed Internet access.[2] The country also boasts a technology-literate general public, and many people carry brand-new smart phones with the latest functionalities. South Koreans are heavy users of social network services ("SNSs") and various other Internet-based services. Along the way, the country has become an immensely information-intensive country.

Considering the development of South Korea's IT infrastructure and the widespread use of SNSs among the general public, it is no surprise that issues related to data privacy have gained particular significance in South Korea in recent years. While South Korea has maintained laws and regulations on data privacy for two decades, the Personal Information Protection Act ("PIPA"), a general omnibus statute governing data privacy matters, was enacted in 2011; since then, issues in data privacy have rapidly gained traction.

In terms of its general structure and major provisions, the PIPA shows similarities to the approach taken in the EU, and both might generally be regarded as leading innovators in developing stringent personal data privacy standards. However, once one begins to examine the relevant legal and regulatory structure in detail, differences can easily be noticed. Perhaps the most noteworthy difference is that, even after the enactment of the PIPA, other data privacy statutes continue to govern certain specific industries or specific types of information such as location information and credit information. Also, multiple government agencies have a role in data privacy matters, each with differing mandates and enforcement authorities derived from different statutes. In light of the range of laws and executive authorities relevant to data privacy in Korea, the general statutory structure and regulatory agencies' enforcement of these statutes should both be examined.

This article will provide an overview of the legal structure regarding data privacy in South Korea and will also examine the jurisprudence that has developed so far. In doing so, certain noteworthy characteristics of South Korea's data privacy law will be delineated, and contrasts will be drawn with other data privacy regimes. In the following section (Section II), the legal and regulatory structure surrounding data privacy in South Korea will be examined, including a review of important features of the relevant statutes. Also, the general enforcement structure of data privacy law will be explained in order to shed light on the overall efficacy of the data privacy regime in South Korea. Then, jurisprudence from court cases will be examined, both to decipher the significance of data privacy on a constitutional level and to clarify the meaning of "Personal Information" and certain other key statutory concepts (Section III). Building on prior sections, Section IV will broaden the analysis by drawing implications for comparative and international aspects of data

1 Ko is Professor at Seoul National University ("SNU") School of Law, Seoul, Korea; Leitner is law clerk for the United States District Court for the District of Maine and Executive Committee member, SNU Center for Energy and Environmental Law and Policy; Kim and Chung are doctoral candidates at SNU School of Law. Ko graciously acknowledges financial support received through the Google Research Awards Program.

2 OECD broadband statistics (http://www.oecd.org/sti/broadbandandtelecom/oecdbroadbandportal.htm). For a journalistic account of South Korea's start-up culture, Amy Guttman, "How South Korea's $3 Billion Bet To Become A Regional Tech Start-up Hub Is Paying Off," Forbes (31 Jan., 2016) (http://www.forbes.com/sites/amyguttman/2016/01/31/why-south-koreas-3-billion-bet-to-become-a-regional-tech-startup-hub-is-paying-off/#4d24dc60a2f9).

privacy law. The article concludes by discussing how Korean data privacy law can be refined to best utilize its distinct features.

2. Legal and Regulatory Structure Surrounding Data Privacy in South Korea

2.1. Placing data privacy in South Korea into context

The PIPA was enacted in 2011 as a general statute governing data privacy issues in South Korea. Prior to the enactment of the PIPA, however, there were already laws and regulations on data privacy in place in South Korea. Perhaps the first data privacy statute in the country was the Public Agency Data Protection Act, which was enacted in 1995. The Act had jurisdiction over data privacy issues in the public sector. In 2001, the Act on the Promotion of Information and Communications Network Utilization and Information Protection ("IC Network Act") was enacted, with various provisions on private sector data privacy. With the enactment of the PIPA in 2011, the Public Agency Data Protection Act was repealed, since the PIPA would serve as a general data privacy statute for both the public and private sectors. However, the IC Network Act was not repealed after the PIPA was enacted, and now generally regulates data privacy issues related to Internet activities.

The PIPA is a comprehensive and omnibus data privacy statute. In terms of its basic structure, it first defines Personal Information, and requires prior notice and consent from data subjects before such Personal Information can be collected and processed.[3] The enactment of the PIPA corresponded with a heightened awareness of the general public regarding the significance of data privacy. Notwithstanding the PIPA's enactment, however, incidents of unlawful data breaches have not decreased. This has led to periodic amendments of data privacy laws. Particularly noteworthy was an incident of massive credit card information leakage, which took place in early 2014.[4] The vast majority of South Korea's adult population was victimized by this incident, and media uproar ensued. This led to major amendments of many of the statutes bearing on data privacy issues. South Korea has adopted very stringent requirements regarding processing of personal information, and the failure to comply with statutory requirements is now subject to heavy criminal and civil penalties.

2.2. The Personal Information Protection Act

As noted, the PIPA is applicable to both public and private sector entities. The PIPA aims to be an omnibus statute governing data privacy, except for situations preempted by specialized statutes. Pursuant to the PIPA, in principle, a "Data Subject" should be given notice and the Data Subject's consent should be obtained before statutorily defined Personal Information can be collected and utilized.[5] "Personal Information" refers to the

3 Personal Information Protection Act, Arts. 2 and 15(1)1.

4 Sang-Hun Choe, 'Theft of Data Fuels Worries in South Korea' The New York Times (New York City, 20 January 2014) <http://www.nytimes.com/2014/01/21/business/international/theft-of-data-fuels-worries-in-south-korea.html> accessed 29 August 2016.

5 [Explain statutory definition of Data Subject, and provide citation.] Personal Information Protection Act, Arts. 2 and 15(1)1.

information about a living person which enables identification of such person, including name, Resident Registration Number,[6] and images.[7] There are exceptions where consent is not required prior to collecting Personal Information, but such exceptions have very limited applicability. More specifically, Personal Information may be collected and processed without consent in the following unavoidable circumstances: when doing so is required by law; when doing so is required to conduct a government's official business; when doing so is needed to form a contract and fulfill the contractual obligations between the Data Subject and the Personal Information Processor;[8] when it is in the Data Subject's clear interests to forego consent; or when it is deemed that the Personal Information Processor's legitimate interests override the Data Subject's interests.[9]

There are other safeguards required as well. For instance, except when separate consent is obtained or when doing so is permitted by law, Personal Information Processors are prohibited from processing "Sensitive Personal Information."[10] Such Sensitive Personal Information includes information on ideology, beliefs, membership in a labor union or political party, political views, health, and sex life. Also, there is a separate category of "Unique Identification Information," comprised of such information as Resident Registration Number, passport number, driver license number, and foreigner registration number.[11] In order to collect the information which belongs to this category, separate consent from the Data Subject should be obtained unless a statutory exception applies. Also, once Unique Identification Information is collected, such information should be encrypted and other technical safeguards should be in place.[12]

In addition to the above, there are requirements that should be fulfilled before Personal Information can be transferred to a third party or before it can cross national borders. Thus, when a Personal Information Processor transfers Personal Information to a third party, in principle, such Personal Information Processor should obtain consent from the Data Subject regarding the transfer.[13] In particular, when the recipient of Personal Information is located outside South Korea, the Personal Information Processor should obtain separate consent from the Data Subject regarding the transborder transfer.[14]

While consent plays a crucial role regarding permissibility of collecting and processing Personal Information, a Data Subject is given certain control rights over the Personal Information even after granting consent. First, a Data Subject has a right to access the Personal Information collected.[15] Also, a Data Subject can make a request to correct the Personal Information if the information that the Personal Information Processor holds is

6 Virtually all residents in South Korea are given unique numbers called Resident Registration Numbers. Until recently these numbers have been widely used as a form of identification by institutions in both the public and private sectors.
7 Personal Information Protection Act, Art. 2(1).
8 Personal Information Processor, as defined in Article 2(2) of the PIPA, is an administrative body, legal person, association or individual which processes personal data directly or indirectly to utilize it. This concept can generally be understood as encompassing both the Data Controller and Data Processor concepts within the EU data privacy regulation framework.
9 Personal Information Protection Act, Arts. 15(1)2 through 15(1)6. It appears that some of these provisions have rarely been used in practice. For instance, although consent is not required when the Personal Information Processor's legitimate interests override the Data Subject's interests, it is not clear who is authorized to make the decision on the applicability of this provision. The meaning of "legitimate interests" is unclear as well.
10 Personal Information Protection Act, Art. 23.
11 Personal Information Protection Act, Art. 24(1).
12 Personal Information Protection Act, Art. 24(3).
13 Personal Information Protection Act, Art. 17(1)1.
14 Personal Information Protection Act, Art. 17(3).
15 Personal Information Protection Act, Art. 35(1).

incorrect.[16] Further, a Data Subject can make a request to stop further processing of his or her Personal Information.[17] Upon receiving these requests, Personal Information Processors are obliged to comply.[18]

Overall, the PIPA contains many features which arguably reflect the general trend that is emblematic of modern data privacy statutes. The PIPA, in particular, explicitly incorporates the eight major principles stipulated in the OECD's privacy guidelines, which laid a foundation for modern data privacy regulations.[19] That is, Article 3 of the PIPA lists basic principles of data privacy that were derived from the OECD guidelines, with some modifications. In terms of its general statutory structure, and given that the PIPA is an omnibus data privacy statute, it shows many similarities to the EU's Data Protection Directive or the General Data Protection Regulation.[20]

At the most fundamental level, similar to the general approach taken in the EU and in certain statutes in the U.S.,[21] the PIPA defines Personal Information and requires consent prior to collecting such Personal Information. At the same time, there are differences as well. One notable characteristic of the PIPA is that it places a particular emphasis on Data Subjects' consent.[22] Thus, for instance, unless exceptions apply, obtaining consent is a crucial pre-requisite for transborder transfer of Personal Information. With consent, Personal Information can cross borders without limitation and, in principle, there is no room for regulators to intervene regarding transborder flows of Personal Information. This is in contrast to the EU approach, under which regulators are expected to play a more active role, whether or not individuals have consented to information transfers. In the EU, transborder transfer of personal information can be made, among others, to the countries with an "adequate level of protection," without having to obtain Data Subjects' consent.[23] The decision as to whether a country provides an adequate level of protection is made by the regulatory authority.[24]

Also, the data privacy regulator's role under the PIPA is different from what is expected from a Data Protection Agency ("DPA") under the EU approach. Within the EU, a DPA in each member country generally assumes various specific roles related to data privacy, including in particular as a regulatory enforcer of data privacy law. The Personal

16 Personal Information Protection Act, Art. 36(1).
17 Personal Information Protection Act, Art. 37(1).
18 Personal Information Protection Act, Arts. 36(2) and 37(2).
19 Organization for Economic Cooperation and Development (OECD), OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, OECD Doc. C(80)58/final (original version, 1980). In 2013, the OECD published a revised version of these original OECD guidelines which adopted the same eight privacy principles. [cite 2013 document]
20 Principles set forth in Article 3 of the PIPA are generally analogous to the principles that are found in Article 5 of EU's GDPR.
21 In the U.S., the statutory requirement to obtain prior written consent for the disclosure of personal information dates back at least to the Privacy Act of 1974, although the requirement in that statute applies only to government entities that collect personal information and is limited by express exceptions and by certain exemptions. 5 U.S.C. Sec. 522(a). Other federal laws on the collection of certain types of personal information generally only require notice of the collection practices, and in some cases a statutorily mandated opt-out. ***See, e.g.,*** Children's Online Privacy Protection Act (opportunity for parents to opt out of collection of personal information on a child under 13 years of age), Gramm-Leach-Bliley Act (financial institutions must provide opportunity for individuals to opt out of the sharing of their personal information with non-affiliated third parties).
22 Mainly due to this strict adherence to the consent principle, data brokers are all but non-existent in South Korea.
23 Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data [1995] OJ L 281/34.
24 [Provide statutory citation]. The negotiation of the Privacy Shield between the U.S. Department of Commerce and the European Commission provided a vivid recent illustration of the EU's centralized regulatory leverage in defining the terms under which the PI of EU persons can be transferred outside of the EU. Annexes to the Commission Implementing Decision pursuant to Directive 95/46/EC of the European Parliament and the Council on the Adequacy of the Protection Provided by the EU-U.S. Privacy Shield.

Information Protection Commission ("PIPC"), the main regulatory agency under the PIPA, however, lacks enforcement authority. Instead, as explained below, multiple government agencies play supplemental roles in order to make sure that data privacy laws and regulations are complied with.

2.3. Other Data Privacy Statutes

While the PIPA serves as a general statute governing data privacy matters, there are other relevant laws as well. These laws exercise jurisdiction over specific sectors or issues.[25] In that respect, South Korea's data privacy regime can be called a hybrid regime between the EU model of omnibus data privacy legislation and the sectoral approach of the U.S. South Korea's sector-specific statutes include the IC Network Act, the Act Concerning the Protection and Utilization of Location Information ("Location Information Act"), and the Act Concerning the Protection and Utilization of Credit Information ("Credit Information Act"). The main features of these statutes are summarized below.

2.3.1. IC Network Act

The IC Network Act is applicable to data privacy issues involving information and communication service providers, and thus it covers a significant part of online activities. In terms of its statutory structure and general overarching principles on data privacy matters, the IC Network Act shares much in common with the PIPA. Thus, similar to the PIPA, the IC Network Act provides that a User should be given notice and his or her affirmative consent should be obtained before Personal Information can be collected and processed.[26] Also, similar to the PIPA, the IC Network Act provides for an additional layer of protection for certain types of Personal Information. That is, unless separate consent is obtained or doing so is permitted by law, collection of sensitive information is prohibited. Personal Information which belongs to this category would include the information which, if breached, is likely to infringe upon individuals' rights and privileges or upon private life, such as information on ideology, beliefs, family relationship, education, and health.[27]

Furthermore, the IC Network Act restricts the transfer of Personal Information to a third party, which is again similar to the PIPA. Thus, transfer of Personal Information to a third party requires consent from Users.[28] In addition, separate consent is required for the crossborder transfer of Personal Information.[29] In terms of granting opportunities to access and to make a request for corrections, similar rights are provided for in both the IC Network Act and the PIPA.[30]

There are, of course, differences between the IC Network Act and the PIPA. However, in terms of general statutory structure and enforcement mechanisms, the differences are

25 Regarding the issue of precedence, Article 6 of the PIPA stipulates that PIPA prevails "unless any other law has a special provision on the protection of personal data."
26 IC Network Act, Art. 22(1). Both the PIPA and the IC Network Act use the term "Personal Information," and its definition is virtually the same in both statutes. Regarding the individual whose Personal Information is at issue, the term "User" is used in the IC Network Act, whereas as the same individual would be called a Data Subject under the PIPA.
27 IC Network Act, Art. 23(1).
28 IC Network Act, Art. 24-2(1).
29 IC Network Act, Art. 63(2).
30 IC Network Act, Art. 30.

minute. In practical terms, perhaps the most significant difference is that the IC Network Act is applicable to information and communication service providers and thus covers much online activity, whereas the PIPA would mostly apply to offline activities. In addition, the regulatory authorities are different. The Korea Communications Commission ("KCC") enforces the IC Network Act,[31] while the PIPC and the Ministry of the Interior are the primary executive enforcement bodies for the PIPA.[32]

2.3.2. Location Information Act

The Location Information Act regulates issues related to location information. This law was promulgated in 2005, several years before the PIPA was enacted. Personal Location Information, as defined in the Location Information Act, refers to the information which can be collected through communications equipment and which would enable a person to be located.[33] As such, Personal Location Information is conceptually different and distinct from Personal Information. At the same time, however, Personal Location Information is closely related to Personal Information since the location information of an individual may, in many circumstances, possibly be linked to the identity and identifiability of such individual, and may give rise to inferences about certain additional Personal Information of the individual.[34] The KCC administers the Location Information Act.

The general statutory structure of the Location Information Act is similar to that of the PIPA or of the IC Network Act in that it employs a stringent notice-and-consent requirement. That is, the Location Information Act requires providers of location-based services to obtain consent from Personal Location Data Subjects before collecting and utilizing Personal Location Information.[35] Further, transfer of Personal Location Information to a third party requires consent from Personal Location Data Subjects.[36]

2.3.3. Credit Information Act

The Credit Information Act is a specialized statute, applicable to personal credit information. The notice-and-consent principle is also manifest in the Credit Information Act and thus, unless exceptions apply, consent must be obtained prior to collecting and utilizing personal credit information.[37] The Credit Information Act prohibits collection of information on private life that is deemed unrelated to personal credit, such as the information on religion and political views.[38] The Credit Information Act additionally contains provisions regarding the mechanisms as to how public credit registers and credit bureaus can collect and share credit information.[39] The Credit Information Act imposes heavy

31 [Provide statutory provisions]
32 [Provide statutory provisions]
33 Location Information Act, Art. 2. The same article also defines such terms as Personal Location Information, and Personal Location Data Subject, which would correspond to Personal Information and Data Subject, respectively.
34 *See* Bellovin, Steven M., et al., ***When enough is enough: Location tracking, mosaic theory, and machine learning***, NYU J. L. LIBERTY 8, 556 (2013).
35 Location Information Act, Art. 15(1).
36 Location Information Act, Art. 19(2).
37 Credit Information Act, Art. 15(2).
38 Credit Information Act, Art. 16(1)3.
39 With the recent amendment of the Credit Information Act, public credit registers were consolidated into one single entity. Credit Information Act, Art. 25(2). There are several credit bureaus, two of them being dominant in the market.

restrictions regarding sharing of customers' credit information among the affiliated financial institutions of a single financial holding company.[40] The Financial Services Commission and Financial Supervisory Service are the main regulators in charge of administering the Credit Information Act.

2.4. Enforcement Mechanisms

As noted above, in addition to the PIPA, there are other sector-specific statutes in South Korea and, as such, different regulatory agencies are in charge of enforcing different statutes. In terms of enforcing data privacy statutes, there are three primary categories of remedial routes. First, government agencies could order corrective measures and impose administrative fines. Second, there are possibilities of criminal penalties since many statutes contain provisions providing for criminal liability for violations. Third, victims of data breaches or other injured parties can of course bring civil lawsuits in pursuit of monetary damages for negligence.

2.4.1. Administrative proceedings

While the PIPC specializes in data privacy matters, it lacks investigative and enforcement authority. Thus, for instance, it cannot impose administrative fines for infractions. It is nonetheless authorized to make resolutions on various data privacy matters.[41] The PIPC may also make recommendations to governmental agencies pertaining to agency violations of the PIPA.[42] Further, the PIPC has a mandate to prepare and submit an annual report on data privacy to the National Assembly, South Korea's legislature.[43] The PIPC does not function as an enforcement agency, and in practice, much of the enforcement role falls to the Ministry of the Interior, which is authorized to impose administrative fines and to order corrective measures.[44] The Ministry also has the authority to file criminal complaints if there is a serious infraction of the PIPA and to recommend reprimanding civil servants who have violated the PIPA.[45] Further, the Ministry of the Interior is authorized to issue standards and guidelines on various issues in data privacy.[46] Perhaps reflecting the breadth of authority granted to the Ministry of the Interior on data privacy matters, it maintains a separate bureau mostly dealing with data privacy matters, the Personal Information Protection Policy Bureau. This Bureau, in turn, has 4 divisions under its auspices.[47]

The KCC is also a major government agency that deals with data privacy matters: it has enforcement authority based on the IC Network Act and also on the Location Information Act. With the recent amendment of the IC Network Act, the amount of administrative

40 [cite provision]
41 More specifically, the PIPA lists twelve itemized data privacy matters about which the PIPC has authority to deliberate and prepare resolutions. These include the improvement of policies, systems, laws and relevant regulations concerning the protection of private information, the coordination of opinions among public institutions with regards to the management of personal information, and the interpretation and application of laws and relevant regulations concerning the protection of personal information. Personal Information Protection Act, Art. 8(1).
42 Personal Information Protection Act, Art. 64(4).
43 Personal Information Protection Act, Art. 67.
44 Personal Information Protection Act, Arts. 34-2(1) and 64(1).
45 Personal Information Protection Act, Art.65.
46 Personal Information Protection Act, Art. 12.
47 Although it is a too simplistic comparison, having a separate bureau with four divisions can be compared to the organization of the PIPC, which has only three divisions in whole. [See if PIPC's annual report shows the number of personnel at the PIPC.]

fines that the agency can impose increased significantly. For major violations of the IC Network Act, the KCC now can impose up to 3% of the "relevant" sales revenue as administrative fines.[48] Violations of the Location Information Act could also result in administrative fines of up to 3% of the relevant sales revenue.[49] On the other hand, in the realm of financial services, the Financial Services Commission ("FSC") is the main agency in charge, administering the Credit Information Act. Again, with the recent amendment of the Credit Information Act, the FSC can now impose up to 3% of the relevant sales revenue if there are violations of the Credit Information Act.[50]

From the above description and recent experiences in South Korea, the following can be said about government agencies' enforcement efforts. First, there are multiple government agencies with distinctive and supplementary mandates to enforce data privacy laws and regulations. Second, efforts have been made in recent years to streamline and reduce inconsistencies among different statutes, while at the same time reinforcing penalty provisions. The amount of the maximum administrative fines is a good example, as 3% of relevant sales revenue is the typical figure following recent statutory amendments. Third, many government agencies have recognized the significance of data privacy matters and have tried to increase their budget and personnel devoted to data privacy.

2.4.2. Criminal proceedings

Many of the statutes dealing with data privacy matters, including the PIPA, the IC Network Act, the Location Information Act, and the Credit Information Act, contain provisions allowing for criminal punishment of data breaches and other violations.[51] Possible criminal sanctions include not just criminal fines but also imprisonment. The availability of criminal punishment plays an important practical role in enforcing data privacy in South Korea. The mere possibility of criminal punishment may have a significant deterrent effect on potential violators. More to the point, the availability of criminal punishment also implies that the prosecutors' office and police often assume the role of de facto investigators and enforcers of data privacy matters. That is, the prosecutors' office and/or police sometimes instigate their own investigations and bring criminal charges, independent of any administrative or civil proceedings. Such criminal charges, in turn, are often followed by administrative proceedings and civil lawsuits.

2.4.3. Civil lawsuits

Private parties can bring lawsuits seeking damages or other civil remedies if there are data breaches or other violations of data privacy law. For such lawsuits, in general, compensatory damages as well as moral damages may be awarded. In recent years, efforts have been made to streamline the overall procedure and to reduce the entry barriers for plaintiffs when they seek damages. That way, it was hoped that victims of data breaches and other infractions would be incentivized to bring civil lawsuits. Thus, with the 2014

48 IC Network Act, Art. 64-3(1).
49 Location Information Act, Art. 14(1).
50 Credit Information Act, Art. 42-2(1).
51 Personal Information Protection Act, Arts. 70 through 74-2; IC Network Act, Arts. 70 through 76; Location Information Act, Arts. 39 through 42; and Credit Information Act, Arts. 50 and 51.

amendment of the PIPA, punitive damages in the amount up to three times the substantiated harm may be awarded, provided that the Personal Information Processor was grossly negligent or failed to show a lack of intent.[52] Further, statutory damages are now available up to 3 million Korean Won (approximately 2,500 U.S. Dollars), with no requirement on the part of plaintiffs to substantiate the actual harm suffered, provided that the Personal Information Processor was negligent or had intent to cause harm.[53] The burden of proof to substantiate that the Personal Information Processor was at fault or negligent is shifted from the plaintiff to the defendant.[54] In terms of the general civil procedure, in order to ameliorate the burden for small-claim plaintiffs, a "group lawsuit" was also introduced, by which a consumer organization or not-for-profit civic group is allowed to bring a lawsuit on behalf of the individuals who suffered privacy harms.[55]

2.4.4. Prospects

Overall, civil remedies have not played a crucial role so far in promoting compliance with data privacy laws. Similarly, it is doubtful that administrative sanctions have served as an effective tool in preventing and containing massive data breach cases or other serious infractions, although regulatory agencies have been diligently issuing guidelines and rendering corrective orders. Facing these criticisms, as summarized above, laws were amended in recent years to make it easier for victims to file a lawsuit and to obtain civil damages and, at the same time, the maximum amount of administrative fines was significantly increased. It remains to be seen whether recent amendments of the laws will have a meaningful impact.[56]

3. Jurisprudence on Data Privacy in South Korea

3.1. Constitutional dimension

Rights to data privacy are not explicitly stated in South Korea's Constitution. The country's Constitutional Court, however, declared that data privacy rights are constitutional rights through a ruling in a Constitutional Court case in 2005.[57] This case, commonly referred to as the Fingerprint case, raised a question about the constitutionality of requiring fingerprints from virtually all adult Korean citizens in the process of issuing national Resident Registration Cards and of utilizing the fingerprint information thus collected when the police conducts criminal investigations. The Constitutional Court acknowledged that data privacy rights are not specifically set forth in South Korea's Constitution. The Constitutional Court, however, reasoned that data privacy rights should nonetheless be recognized as fundamental constitutional rights, which are derived from other rights that are

52 Personal Information Protection Act, Arts. 39(3) and (4). Punitive damages are available under the Credit Information Act as well. Credit Information Act Art. 43(2).
53 Personal Information Protection Act, Art. 39(2). Statutory damages were recently introduced to the IC Network Act and the Credit Information Act as well. IC Network Act, Art. 32-2(1); and Credit Information Act, Art. 43-2(1).
54 Personal Information Protection Act, Art. 39(1).
55 Personal Information Protection Act, Art. 51. While "class action" lawsuits are not generally permitted in civil litigation in Korea, PIPA provides a particular exception. The National Assembly's action can thus be seen to acknowledge the special challenge posed by the widespread but difficult to quantify harms of privacy law violations.
56 [Notwithstanding recent legal amendments, there are skeptics.]
57 Constitutional Court of Korea, 99hunma513, 2004hunma190, decided 26/5/2005.

explicitly stated, such as the right to private life (Article 17) and the right to dignity and to pursue happiness (Article 10). The Constitutional Court further clarified that the "right to information self-determination" is the most crucial aspect when data privacy rights are concerned. From this reasoning, the Constitutional Court ruled that fingerprints are personal information and that an act of collecting and utilizing fingerprint information constitutes a restriction on the "right to personal information self-determination."

The Constitutional Court's decision was rendered prior to the enactment of the PIPA. Nonetheless, this case is cited repeatedly as a leading case concerning data privacy. In particular, through this case, the Constitutional Court declared, for the first time, that data privacy rights are fundamental constitutional rights and that the right to self-determination is the most crucial aspect of data privacy rights. The PIPA's emphasis on affirmative consent and opportunities for individuals to actively influence the content, use, and processing of their Personal Information is best understood in this context. The PIPA did not displace subject-specific privacy laws, but it nonetheless provides a coherent attempt to codify the data protections necessary to vindicate the emerging constitutional understanding of personal privacy rights.

In a more recent ruling rendered in 2015, the Constitutional Court affirmed its position that data privacy rights are constitutional rights and that, as such, the right to information self-determination should be well-respected.[58] Rendering its decision for the Resident Registration Number case, the Constitutional Court ruled that South Korea's national Resident Registration Number system should provide a procedure allowing for possibilities of changing Resident Registration Numbers in the event that a legitimate need arises for such changes and should thereby guarantee Koreans the right to information self-determination.

There is now little doubt that, in South Korea, data privacy rights must be treated as fundamental constitutional rights and that, as such, the right to information self-determination has constitutional significance. Other data privacy rights may be derived from this constitutional foundation. These derivative rights would include the right to demand access to one's Personal Information and the right to demand suspension, correction, and destruction of the processing of Personal Information.[59]

3.2. Definition of Personal Information

Defining "Personal Information" in relevant statutes is critically important in discussing data privacy in South Korea. This is so because once a piece of information is legally construed to be Personal Information, notice, consent and other stringent legal requirements begin to apply before collecting and processing of such information can be permitted. On the other hand, notice and consent requirements do not apply to the information that is not deemed Personal Information and, therefore, it is much easier and less burdensome to collect and process the information that is not Personal Information. As noted,

58 Constitutional Court of Korea, 2013hunba68, decided 23/12/2015.

59 Personal Information Protection Act, Art. 4. The PIPA's identification and protection of derivative data privacy rights indicates that, at a minimum, lawmakers have sought to embody the spirit of constitutional privacy law in the Civil Code, and may suggest an interplay between the courts and the legislature in developing the scope of constitutionally necessary data security regulations.

the PIPA defines Personal Information as information which enables identification of a person.[60] More importantly, to be considered Personal Information under this statutory definition, identification needs to be possible either directly or indirectly, that is, (1) directly using the given information at hand or (2) indirectly when "easily combined" with other information.[61] Thus, not just direct identification but also indirect identification, if identifying becomes possible when a dataset is "easily combined" with other datasets, could meet this definition.

In practice, how to apply this statutory definition can easily become a very contentious issue. There have been two lower court cases where the judiciary in South Korea was asked to render its decision on this issue. The first of these two cases, the IMEI case, concerned a developer of a smart-phone application for instant stock-price quotations who obtained users' IMEI (International Mobile Equipment Identity) and USIM (Universal Subscriber Identity Module) information in the process of app installation.[62] With the IMEI and USIM information, the app developer could identify and remember a user's smart phone and was able to provide tailored quotation services to app users, reflecting individual app users' search history. Certain further information would be needed to identify not just the device but also the user, since the IMEI and USIM information would allow the identification of a user's phone but would not reveal the user's identity per se.[63] Thus, for instance, if the subscriber data that mobile carriers hold can possibly be accessed, such subscriber data could easily be linked and combined with the IMEI and/or USIM information to identify the user. This is because the subscriber data would contain such information as a subscriber's name, date of birth, address, and billing information, as well as certain device-related information (including IMEI and USIM). On the other hand, a smart phone's IMEI and USIM would not contain the device user's name or other information that could easily be deemed Personal Information.

In this context, a more practical issue is whether the app developer could somehow gain access to a mobile carrier's subscriber data legitimately and whether, that way, such subscriber data can possibly become accessible. In all likelihood, getting access to a mobile carrier's subscriber data in any legal manner would be hard to imagine. Nonetheless, the Court held that the IMEI and USIM information should be considered Personal Information. The Court's reasoning was that it was not necessary to consider whether the app developer could obtain the subscriber data held by mobile carriers and that it was only necessary to consider whether, if such subscriber data somehow became available, the app developer could without difficulty identify the app's users. The Court ruled that the IMEI and USIM information is Personal Information since, in the event that the app developer could obtain a mobile carrier's subscriber data, the app developer would easily be able to combine the subscriber data with the app user data in order to figure out users' identity.

The other case where the Court was asked to interpret the statutory definition was the

60 Personal Information Protection Act, Art. 2.
61 Personal Information Protection Act, Art. 2. The IC Network Act defines Personal Information in a similar manner. IC Network Act, Art. 2.
62 Seoul Central District Court, 2010godan5343, decided 23/2/2011.
63 More precisely, the IMEI information can be used to identify an individual smart phone device, while the USIM information can be used for the identification of an individual USIM card which is inserted in a smart phone.

Mobile Phone Number case.[64] In that case, the issue was whether the last four digits of a mobile phone number should be considered Personal Information under the PIPA. With the last four digits of a mobile number, could an identification be easily made? In a case where there is further information that can be linked to a particular four digit number for a mobile phone, identification can perhaps take place very easily. For instance, if it is known that an individual who uses a particular set of four digits is someone's acquaintance and that they both know each other's phone numbers, identification can be done extremely easily simply using the search function of a mobile phone's directory. On the other hand, if there is no such additional information, identifying someone simply from a four digit number could be a fairly cumbersome process.[65] In this particular lawsuit, the Court ruled that the last four digits are Personal Information. The Court simply reasoned that, given the four digits of a mobile phone number, identification of an individual who uses the four digits for his or her own mobile number can be carried out without much difficulty.

For both of the cases introduced above, the cases did not reach the appellate level. If the court's line of reasoning is followed, virtually any information related to individuals can be considered Personal Information. Naturally, there are critics who argue against such a broad interpretation of the statutory provision.

3.3. Lawsuits from data breaches

In relative terms, there have not been many lawsuits filed so far in South Korea related to data privacy matters. Among these lawsuits, the issues of negligence and the resulting damages in data breach cases have arisen repeatedly. A number of large-scale data breach incidents have produced lawsuits through which the Korean courts have set forth criteria for determining negligence and, if negligence is established, the amount of damages to be awarded.

Among the cases that were brought in this context, few reached the Supreme Court level. One of these cases involved Auction, a popular e-commerce site.[66] The server of this e-commerce site was hacked in 2008, and a massive amount of user information was breached, including the names, Resident Registration Numbers, account numbers, and addresses of the site's users. Information on over 10 million users was leaked and, among these users, approximately 146,600 users brought lawsuits against the company, claiming damages for negligence. The case eventually reached the Supreme Court, which reasoned that various factors need to be considered in a data breach case such as the status of technical developments for Internet security at the time of hacking, the security measures that were in place at the time of hacking, and the actual technical tools that were used by the hackers. The Supreme Court ruled that, considering these factors, Auction did what was reasonably expected to be done to prevent data breach and thus could not be held liable for negligence.

64 Daejeon District Court, 2013godan17, decided 9/8/2013.

65 In South Korea, a mobile number is composed of 11 digits. Of these, the first three digits are the same for most numbers (i.e., "010"). Thus, in ordinary circumstances, if four digits of a mobile number are given, there are additional four digits to figure out in order to identify an individual. This means that there are roughly 10,000 possible combinations, and confirming and identifying an individual from 10,000 combinations could certainly be done with some degree of time and effort.

66 Supreme Court, 2013da43994, decided 12/2/2015.

Another Supreme Court case involved the bonus membership system maintained by a major oil retail company, GS Caltex, and one of its subsidiaries.[67] An employee of this subsidiary obtained the membership database, prepared a CD containing the information on members although he was not authorized to do so, and tried to disseminate the information for monetary gain. Before the membership information was disseminated, however, the employee's scheme was uncovered, and the information was never actually made publicly available or transferred to other parties. Subsequently, subscribers to the bonus membership brought a civil lawsuit against the oil company, and the case reached the Supreme Court level. The Supreme Court noted the fact that the personal information at issue was after all not disseminated to third parties, and that as such no personal information was disclosed against the will of the membership subscribers. Thus, the Supreme Court ruled that no damages, compensatory or moral, could be awarded.

While plaintiffs were unable to obtain damages in the above two cases, there are certain lower court cases where the court awarded damages for negligence in data breach cases. One such case involved a job application website maintained by a large conglomerate company.[68] A job applicant to the company obtained application materials of all the other applicants from the company website and, soon afterwards, some of the information contained in these application materials began spreading through various Internet bulletin boards. Some of the job applicants whose information was disseminated brought claims against the company, and the Court awarded damages in the amount of 300,000 Korean Won (approximately 250 U.S. Dollars) per person. In another case, a bank employee sent group e-mails to certain account holders and, in doing so, inadvertently attached a file containing the information on the account holders' names and Resident Registration Numbers.[69] Some of the account holders brought a lawsuit against the bank. The Court held that the defendant was negligent and awarded damages ranging between 100,000 and 200,000 Korean Won (approximately between 80 U.S. Dollars and 160 U.S. Dollars) for each plaintiff.

Separate from the data breach cases mentioned above, recently, other types of cases began to emerge, which go beyond data security and instead involve more fundamental data privacy issues. One such case involved a sweepstakes event held by Home Plus, a major retail chain store of household merchandise. In return for the possibility of sumptuous prizes, participants were asked to submit their contact information and other personal information, which would then be sold to certain insurance companies for marketing purposes. Consent had been obtained from the participants, but legal challenges were made about the validity of such consent. Among other arguments, the allegation was made that the consent form used was a standard form contract with exceedingly small-sized font, which rendered the consent form practically illegible. This raised a novel question as to the valid and legitimate means of giving notice and obtaining "informed consent" in the context of South Korea's data privacy law. That is, this case raised a question as to whether use of a small-font standard form was inadequate for notice and consent purposes and, if so, what documentation would be legally sufficient.

67 Supreme Court, 2011da59834, 59858, 59841, decided 26/12/2012.
68 Seoul High Court, 2008na25888, 25895, 25901, decided 25/11/2008.
69 Seoul High Court, 2007na33509, decided 27/11/2007.

This case also raised an important question regarding the overall regulatory and enforcement structure of data privacy in South Korea. Soon after the sweepstakes drew media attention, the Korea Fair Trade Commission, a competition law regulator with a mandate to regulate standard form contracts, proceeded with formal charges against the company for violating the Standard Form Contract Act and imposed an administrative fine in the amount of [ ].[70] Separately, the Supreme Prosecutors' Office brought criminal charges for violations of the PIPA,[71] and civil lawsuits are also pending in pursuit of damages.[72] Thus, several different types of legal proceedings based on this single incident have taken place concurrently or in sequence.[73]

In another case, the court was asked whether South Korea's data privacy laws would permit sharing of Personal Information if the information is encrypted.[74] A civil lawsuit, arising out of the same set of incidents, was brought in 2014 against the Korean Pharmaceutical Association, the Korean Pharmaceutical Information Center, and IMS Health Korea. A principal allegation was that the Korean Pharmaceutical Association and the Korean Pharmaceutical Information Center collected prescription information and other personal health information of a massive number of outpatients who visited medical clinics without obtaining consent from these outpatients. It was also alleged that the collection of personal health information was made using a networked software system installed on pharmacy computers and that much of the personal health information thus collected was unlawfully transferred to IMS Health Korea and was subsequently sold to various pharmaceutical companies after being repackaged and analyzed.[75]

The ruling in this case will have a significant impact on data privacy jurisprudence in South Korea and also on the future path of the data industry. In particular, the Court decision on this case will have a strong influence as to whether the data brokerage industry can legitimately conduct business in South Korea, notably in the health and pharmaceutical industries and, if so, what kinds of safeguards will be needed, including the technical complexity of encryption required.[76]

4. Critical assessment of Korean data privacy implementation

The overall structure of the PIPA in South Korea looks, on its surface, to be similar to the EU's framework of data privacy. This is not surprising considering that, in recent years, so

70 [Provide citation]

71 District court decision was made on [ ], which held that Home Plus was not liable. [cite case number] Appeal is currently pending at the [ ] Court. [cite case number]

72 [Provide citation] [Summarize the current status of legal proceedings]

73 The Prosecutors' Office tends to assume a proactive role, bringing charges more expeditiously than administrative or civil proceedings progress. Whether compliance and heightened public awareness would be advanced if multiple institutions almost simultaneously engaged in legal proceedings is an important question that lies beyond the scope of this article.

74 Seoul Central District Court, 2014godan5110, pending. One of the authors of this article served as an expert witness for this case.

75 The case is pending at the District Court level at the time of writing this article. Fact summary of the case is mostly from 2014 Form 10K for IMS Health Holdings. IMS Health Ltd. 2014 (http://ir.imshealth.com/files/51a1975c-604b-4a89-b19b-6d36fa633e19_v001_g8065f.pdf). There is a separate criminal case against former president of the Korean Pharmaceutical Information Center, which is pending at the District Court level too. [CONFIRM ACCURACY] [Provide citation]

76 Currently, there are virtually no data broker companies in South Korea, due in significant part to exceedingly stringent individual consent requirements.

many countries enacted data privacy laws generally modelled after the EU approach.[77]

At the same time, there are nuanced and significant differences.[78] In this section, we will review certain characteristics of South Korea's data privacy law which can arguably be differentiated from the approaches found in many other jurisdictions and will try to draw implications in the context of current international discussions for enhancing compatibility between Korea and other data privacy regimes, most notably the EU and the U.S.

When engaging in comparative analyses, de facto law often matters as much as, if not more than, the de jure law.[79] Law in practice is particularly important in the realm of data privacy law, since relevant statutes have been in place for only a few years in many countries and, at most, for a few decades. However, attaining a clear view of legal practice realities is not an easy task, because different countries have different legal and regulatory systems and also because useful data are rarely available. Nonetheless, instead of relying upon a comparative analysis of statutory provisions to reach a conclusion as to convergence or divergence, we attempt a comparison of the implemented features of data privacy practice across jurisdictions.

Our comparison is conducted at a more granular level based on four factors that Paul Schwartz recently proposed.[80] The first factor is to evaluate different legal institutions for policing data privacy in different legal systems. The second factor is an examination of the kinds of harms that are considered as relevant in a legal dispute involving data privacy. The third considers the enforcement mechanisms for data privacy that are in place. The fourth looks at the impact of technology as a practical regulatory apparatus.

First, regarding institutions, relevant institutions on data privacy in South Korea include the National Assembly, the PIPC, the Ministry of the Interior, the KCC, the Prosecutors' Office, the Police, and the Judiciary.[81] In its early privacy legislation, the National Assembly delegated technical details to technocrats and outside advisers. In recent years, however, as data privacy violations have received an increasingly high level of public attention, many legislators began paying close attention to data privacy issues. The judiciary, in relative terms, has played a limited role in enforcing data privacy law. Judges as a class have been criticized by some as too reluctant to award a large amount of damages in data breach cases. Even if one can assume that judges can be labelled as reluctant in this regard, a devoted study would be required to determine whether such reluctance is due to their general proclivity or due to the lack of legal grounds which would justify larger damages awards. In particular, considering the recent overhaul of statutory provisions on damages assessment and the burden of proof, it remains to be seen if recent legal amendments will have a significant impact. As for regulatory agencies, there simply is no "one-stop shop," limiting the ability of any agency to provide consistent and rigorous

77 Graham Greenleaf, Asian Data Privacy Laws, Trade and Human Rights Perspective (Oxford University Press 2014). According to Greenleaf, the EU approach has now become a ***de facto*** global standard.

78 For instance, Korea has certain statutes regulating data privacy issues in specific sectors, as in the U.S. One prominent example is the Credit Information Act, which governs data privacy issues in the financial industry.

79 For an example of research that emphasizes the importance of reviewing what is happening in reality, see Kenneth Bamberger and Deirdre Mulligan, Privacy on the Ground: Driving Corporate Behavior in the United States and Europe (MIT Press 2015).

80 [Cite Schwartz, Comparative Contractual Privacy Law: The U.S. and EU]

81 Korea Internet & Security Agency, although not a regulatory agency ***per se***, has been playing an important role as well, preparing various reports on data privacy and providing technical and other support to the government.

standards of enforcement. However, in South Korea, government agencies have traditionally played an active role in shaping the law. In the data privacy area, government agencies have indeed been instrumental in drafting statutes and structuring the general landscape regarding data privacy in South Korea.

With recent amendments of data privacy laws, the maximum amount of administrative fines that can be levied increased considerably, and it remains to be seen if these amendments will incentivize stricter compliance. In terms of enforcing data privacy law, the Prosecutors' Office and the Police have been relatively more active in enforcing the law. They have accumulated considerable investigative capabilities, and the fear of criminal penalty serves as a deterrent to potential violators. At the same time, consent from Data Subjects is given paramount significance in collecting and processing data. Once legitimate consent is obtained, Personal Information can freely be transferred to third parties and can also cross national borders. With consent, Sensitive Personal Information can be collected as well, with virtually no further restrictions. To the extent that consent is valid, there is not much room for the regulator to intervene and override the data subject's decision in this context.

The second assessment factor is related to the issue of assessing harm. South Korean courts recognize compensable harm from data privacy violations. There is even a constitutional foundation to data privacy rights. However, damage awards have been limited to those persons whose personal information is proven to have been disseminated to third parties. Thus, even if there is a data breach incident, data subjects may not be granted damages if the stolen data were recovered before being disseminated to third parties.[82]

The third factor concerns enforcement. As noted above, legal remedies, in particular in the form of damages or administrative fines, have been weak in South Korea.[83] The modest amount of damages can be understood to be in line with the amount that would be available in other types of comparable civil damages. Regarding administrative fines, until recently regulatory agencies were simply not authorized to levy a substantial amount of fines. This could potentially change with recent amendments of laws allowing for a relatively large amount of statutory damages, permitting "group lawsuits," and authorizing administrative fines up to 3% of the relevant sales revenue, although any discernable signs of change are yet to appear. Separate from formal sanctions, government agencies have been diligently producing guidelines and providing guidance, which may have the effect of creating practical norms and conventions.

The fourth factor concerns the regulatory power of technology. Many technology companies prioritize collecting data before devoting considerable attention to data privacy issues. This tendency is natural considering that, in network industries, preempting the market and building a large user base is crucial for business success. At the same time, strict laws and regulations, together with uncertainty as to how statutory provisions will be interpreted once disputes arise, would make companies hesitate before engaging in a bold business campaign utilizing information that can possibly be interpreted to be

82 [Explain GS Caltex; and District Court decision in the Home Plus case]

83 Relatively weak regulatory enforcement can be contrasted to South Korea's tough competition law enforcement. For instance, in recent years, the Korea Fair Trade Commission, the nation's competition law authority, levied [ ] to Qualcomm and [give one or two cases with large amounts of fines].

Personal Information. For now, the end result seems to be the general reluctance on the part of the technology community against aggressively engaging in data collection and utilization, although there are occasional cases which serve as a litmus test for delineating boundaries of permissible activities. For instance, as noted, while the data brokerage market is all but non-existent in South Korea, IMS Health Korea has been conducting its businesses allegedly collecting (encrypted) personal health information.

5. Conclusion

Korean data privacy law has rapidly emerged as a strict regime, drawing upon the EU idea of an overarching, central statutory scheme while resembling the U.S. approach in the checkerboard of applicable laws and executive and judicial enforcement bodies. Korea's informed, affirmative consent requirements impose a particularly high bar for users of Personal Information to comply with legal requirements. Recent legal developments, including the Home Plus case, illustrate that informed consent may only be legally effective if individuals understand both the information being used and the implications of their apparent consent. Furthermore, legal reforms have eased procedures for civil actions and imposed significant potential administrative and criminal consequences for violation of data privacy law.

While the trend in Korea has been distinctly in the direction of more restrictive data privacy laws, the full consequences and efficacy of the data privacy laws are less clear. Korea's approach has not yet provided clear and predictable legal and practical standards for commercial actors in fields that rely upon data collection, processing, and sharing. While the laws may limit the emergence of data-based industries, it may not be providing better protection of personal information for individuals. Further, despite Korea's many notice and consent requirements, Koreans may not have better alignment between their preferences and the actual use of their Personal Information.

This article has attempted to provide a broad and contemporary understanding of data privacy law in Korea. By carefully identifying key similarities and differences between the Korean approach and the laws of other jurisdictions, certain issues can be identified that Korean lawmakers and jurists should consider. First, the law should provide clear and meaningful guidance for determining what notice-and-consent procedures and practices can fulfill legal requirements. Legislation and regulations could provide the most clear and standardized guidance. More immediately, courts have the opportunity to apply constitutional requirements and existing statutory language to focus on practical rules for obtaining individual consent. Second, Korean government authorities should seek greater collaboration in the enforcement of data privacy laws. The threat of group litigation, substantial administrative fines, and criminal prosecution may already be constricting commercial activities. However, the lack of clarity about actual consequences of legal violations has contributed to the persistence of data leaks and misuse. Though Korea currently lacks a single governmental body to coordinate enforcement, consistency and predictability should be major goals for making data privacy law more effective.

The Brussels Privacy Hub Working Papers series

The Brussels Privacy Hub Working Papers are intended to circulate research in progress for comment and discussion. The Working Papers focus on all areas of data protection and privacy research and can contain empirical research on privacy issues and analytical work on privacy governance and regulation in the EU; global flows of data; reconciling law enforcement and privacy interests; privacy challenges posed by new technologies; comparative research on privacy in different regions; jurisprudential issues of privacy protection; and many others

Available at www.brusselsprivacyhub.org/publications.html

Contact: info@brusselsprivacyhub.org

N°1 **"The data protection regime applying to the inter-agency cooperation and future architecture of the EU criminal justice and law enforcement area"** (November 2014) by Paul De Hert and Vagelis Papakonstantinou (35 pages)

N°2 **"The new cloud computing ISO/IEC 27018 standard through the lens of the EU legislation on data protection"** (November 2014) by Paul de Hert, Vagelis Papakonstantinou, Irene Kamara (25 pages)

N°3 **"Towards efficient cooperation between supervisory authorities in the area of data privacy law"** (October 2015) by Dariusz Kloza, Antonella Galetta (24 pages)

N°4 "**The data protection regime in China"** (November 2015) by Paul De Hert and Vagelis Papakonstantinou (30 pages)

N°5 **"The right to privacy and personal data protection in Brazil: time for internet privacy rights?"** (February 2016) by Vinícius Borges Fortes (23 pages)

N°6 **"Permissions and Prohibitions in Data Protection Jurisdiction"** (May 2016) by Mistale Taylor (25 pages)

N°7 **"Structure and Enforcement of Data Privacy Law in South Korea"** (October 2016) by Haksoo Ko, John Leitner, Eunsoo Kim and Jong-Gu Jung (20 pages)