온라인 정보보호 및 프라이버시에 관한 국제 표준 개발*

주한나**, 이희진***, 곽주영****, 김용영*****

Data Protection and Privacy over the Internet: Towards Development of an International Standard*

Hanah Zoo, Heejin Lee***, Jooyoung Kwak****, Yong-Young Kim*****

요 약 국경을 넘어선 개인정보의 수집, 처리 및 이전이 일상화되고 있는 가운데, 온라인 정보보호 및 프라이버시에 관한 정책은 크게 두 가지 기조로 나누어지고 있다. EU로 대표되는 인권 기반 접근의 경우 개인의 프라이버시권을 보호하기 위해 기업이 따라야 할 엄격한 요건을 국가가 마련해 부여하고 있는 반면, 다국적 ICT기업이 다수 포진하고 있는 미국의 경우 온라인상의 자유로운 데이터 이동에 초점을 맞춘 업계의 자율규제를 중시한다. 국가 및 지역별로 다르게 나타나고 있는 온라인 정보보호와 프라이버시 정책을 어떻게 조율할 것인가에 대해 두 가지 입장이 상충하는 사례가 잦아지고 있는 상황 속에서, ISO/IEC와 같은 국제 표준화 기구의 합의된 조율 절차를 통해 국제 표준을 개발함으로써 실질적인 해결책을 모색할 수 있다.

주제어 : 정보보호, 프라이버시, 온라인 프라이버시, 표준, 국제 표준화

Abstract Progresses in ICT make the processing and exchange of personal data across international borders often necessary and relatively easy. The challenge lies in protecting fundamental rights and freedoms of individuals, notably the right to privacy and the right to personal information, while encouraging the free and secure flow of information across borders for the continued expansion of online transactions. The key to establishing a functioning international solution for personal data protection is to strike a right balance between the two camps which currently dominate the debate – the advocates of individual privacy rights on one side exemplified by the EU, and the proponents of self-regulation and economic efficiency on the other, represented by the U.S. In the face of a growing tension between the two sides each equipped with their own ideals, a practical solution may lie in utilizing established institutions of standardization such as ISO and IEC as a ground upon which an agreement can take its root.

Key Words : data protection, privacy, online privacy, standard, international standardization

1. Introduction

In September 2012, Facebook announced that it was turning off its facial-recognition tool in Europe. Facebook did so in response to an audit by the Irish Data Protection Commissioner, one of 27 national privacy regulators under the European Union(EU) Data Protection Directive[15].

After the event, the American firm has been openly lobbying the European Commission on the reform of

*This work was supported by the National Research Foundation of Korea Grant funded by the Korean Government (NRF-2011-330-H00002)

**연세대학교 국제학대학원 박사과정
***연세대학교 국제학대학원 교수(교신저자)
****연세대학교 경영대학 교수
*****건국대학교 경영경제학부 조교수

논문접수: 2013년 3월 14일, 1차 수정을 거쳐, 심사완료: 2013년 4월 10일, 확정일: 2013년 4월 20일

"unreasonable and unrealistic" privacy law in EU, notably the Convention of the Council of Europe for the Protection of Individuals with regard to Automatic Processing of Personal Data(Convention 108), but the European Council(EC) Commissioner mentioned that EU will push on stricter measures to protect the privacy of its citizens[5].

On another note, the EU Commission, as recent as December 2012, formally recognized the adequacy of personal data protection in New Zealand, that New Zealand's data protection standards are compatible with those of the EU[6]. The aim of such a decision, according to the EU's Justice Commissioner Reding, is to facilitate the free flow of personal data across borders and thereby boost trade, while helping to set high standards for personal data protection at a global level[6].

The ongoing cases clearly illustrate both the tension and cooperation among countries in the face of a growing trans-border flow of personal data. Indeed, with the advancement of Information and Communication Technology(ICT), international flows of personal information over the Internet have become an integral part of our lives. However, the characteristics of the Internet as a global public good, which operates beyond state borders, pose challenges in the data protection and privacy over the Internet in legal and policy applications. As such, many states have forged divergent national laws and standards on data protection that are not compatible and in some cases, even confront each other.

Against this backdrop, this paper examines major international, regional and national efforts to-date to address the emerging call for a globally applicable personal data and privacy protection initiative, and highlights the characteristics of data protection and privacy over the Internet as a subject of a new, comprehensive international standard. The paper is organized as follows. First, a brief review of previous literature on privacy and data protection over the Internet is presented, including the definition and use of the terms, data protection and privacy, and the key characteristics of trans-border flow of personal information over the Internet. Next, in order to understand the diverse stances taken by states and regional blocs, a selected sample of national and regional policies on data protection is analyzed particularly with regard to their trans-border application. Then, discussions on the perspective of setting up an international public standard on data protection over the Internet is presented.

2. Data Protection over the Internet: Evolution of International Efforts To-date

The advancement of ICT is ever integrating the world in a single networked society. The massive amount of personal data processed globally through Internet-based service transactions is a product of such a change. Capturing its importance in commerce and trade, academic literature has addressed personal data protection as a prerequisite to build trust in the global digital economy. And a growing number of studies examine socio-political issues concerning the personal data protection and privacy[4][11][12][13][14].

Among the studies that address social and political implications of privacy and data protection, which is of particular interest to this research, a major stream of research looks at the issue from the human rights perspective. Particularly, those studies highlight that privacy is a fundamental right recognized in many international treaties and agreements on human rights and in constitutions of many countries around the world, either explicitly or implicitly[14]. For example, the preamble of the Universal Declaration of Human Rights specifically mentions in Article 12 that "*No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to the protection of the law against such*

interference or attacks"[19]. A similar clause is found in the Article 17 of the United Nations International Covenant on Civil and Political Rights[25].

However, with the dominant potentials of technology on personal data over the Internet, the mere recognition of a constitutional principle of privacy in general is now considered insufficient to effectively safeguard the growing need to protect the right of privacy[4]. Reflecting the concern, a number of international policy instruments have been created and adopted during the last three decades. These instruments laid out general principles that a global consensus on the need to protect personal data and privacy should be achieved, taking into account the increasing trans-border flow of personal data over the Internet[11]. Some of the well-known first stage examples include the Guidelines governing the Protection of Privacy and Trans-border Data Flows of Personal Data, promulgated by the Organization for Economic Co-operation and Development(OECD) in 1980[22]; the Convention for the Protection of Individuals with regard to the Automatic Processing of Personal Data adopted by the Council of Europe(COE) in 1981[21]; and the Guidelines concerning computerized personal data files adopted by the United Nations General Assembly in 1980[24].

These policy guidelines, to a certain extent, achieved their political goals. They displayed a common interest to set a minimal level of international standard for data protection, and urged each state to create national legislation and standard to protect online privacy at the national level[13]. Notably, the OECD guidelines have been widely used in national legislation even outside the OECD countries[14]. Moreover, under the technological change, the OECD and COE have continued their efforts, adopting new documents including the COE's recommendation in 1999 for the protection of individuals with regard to the collection and processing of personal data on information highways[20], and the OECD report adopted in 1998 on the implementation of the OECD privacy guidelines in the electronic environment with a focus on the Internet[23].

However, despite the achievement of increased awareness on the importance of privacy protection over the Internet, they have also faced the criticism that these measures are not sufficient as such to safeguard a comprehensive protection in the context of a global networked society[13]. First, since these instruments, mainly in the form of policy guidelines, are limited in their enforceability and scope, the actual level of implementation of data protection policies and their effectiveness differ significantly from country to country. Second, the flexibility these instruments allow has resulted into divergent national laws on data protection. National standards are sometimes found incompatible and therefore, pose a challenge of legal and policy application across state boundaries[14].

Combined together, these setbacks result into a disparity of personal data and privacy protection among countries. For example, the EC Convention as a European standard has a binding force and requires all EC member states to embody the principles of data protection in national law and standards[12]. However, it does not oblige contracting parties which, in a growing number of cases, originate from non-EU member countries, to establish institutional mechanisms for personal data protection[4]. Similarly, the OECD guidelines only carry the requirement that they be 'taken into account' in domestic legislation and provide no means to ensure that the guidelines actually result in effective protection for individuals[13]. Considering that new technologies such as cloud computing and social network service operate ever more globally, such a disparity may present a massive consequence.

By and large, the criticism on the previous instruments of privacy and personal data protection touches on two important issues. First, the international 'policy' instruments so far have failed to provide sufficient protection at the global level, since they have granted too much flexibility for countries to make policy choices regarding how they define the nature

and scope of data protection in national policies. Second, the divergent landscape of national standards for personal data and privacy protection across the globe has not yet been under academic scrutiny, as to what issues – notably political ones – may arise from the ever-increasing trans-border transfer of personal data and how an enforceable international standard on data protection and privacy may affect the matter.

With these two issues in mind, the following sections review the cases of selected regional and national approaches focusing on their respective data protection laws and standards, and discuss their socio-political implications.

3. Regional and National Data Protection Instruments

While the international initiatives to-date have their own values in promulgating the social and political underpinnings for personal data and privacy protection, it is important to narrow down the scope to examine how they are translated into actual policies and implemented as regulatory means in states.

In this regard, two major streams of regulatory measures for data protection warrant further consideration. The extensive approach, often represented by the European system, emphasizes the role of comprehensive governmental regulation that all entities should abide by. The sectoral approach, usually characterized by the American laissez-faire system, focuses on a combination of legislation and self-regulation, rather than government regulation alone. Notably, the tension between the European public institutions with strong data protection requirements and U.S. companies equipped with self-regulatory principles as stated early in this paper, illustrates the two very different approaches.

In the following section, these two major streams will be reviewed with the examples of two regional and two national efforts, the EU and APEC frameworks and the U.S. and Korean instruments, respectively.

3.1 European Union and the Convention 108

In Europe, there is a broad consensus that data protection principles should be embodied in a comprehensive law, applicable to all sectors of the society within the EU system regardless of the national boundary. As such, the European system is considered the strictest[14], which serves as an enforceable regional standard with a possibility to sanction the non-compliance.

To begin with, the COE recognizes the right to privacy as a "fundamental human right." As a result, the European view on the right to privacy tends to address every aspect of the individual's life. Based on this expansive view on the right to privacy, privacy standards in Europe cover the processing of personal data by both the government and private organizations[17]. The COE's Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, also known as the Convention 108, broadly defines personal data as "any information relating to an identified or identifiable individual" and outlines data protection principles, which have served as a basis for data protection standards worldwide[12]. Later, the European Union's Data Protection Directive, which was ratified in 1995, affirmed the Convention's data protection principles, set the standard level of data protection for members of the European Union, and, more importantly, acknowledged the individual's right to privacy[4]. Along with the ratification of the Directive, EU mandated that all current and future member states of the European Economic Area incorporate agreed-by consensus rules into their own respective laws and standards[13].

Such a strong political power exercised by the EU as a regional cooperation mechanism underpins the harmonized, universal approach taken in the Europe beyond the economic interests. In early 2012, the EU unveiled a draft of the European General Data

Protection Regulation, a comprehensive reform proposal which will supersede the current Data Protection Directive and set out its intention to harmonize data protection measures across the EU.

Likewise, the extensive concern over an individual's right to privacy is evident in the treatment of EU's trans-border transfer of personal data. The EU standard allows the transfer of personal data to countries outside the European Union only if the country ensures "*an adequate level of [data] protection*"[12]. Even though the definition of "*adequate level of [data] protection*" is to be determined case by case as "*in the light of all circumstances surrounding a data transfer operation*," the Directive extends the reach of protection afforded to personal data originating in the EU to countries outside its borders[12].

In sum, the Directive's reach has extended past the EU borders, influencing data protection regulation and standard worldwide by forcing other countries to examine their own data protection legislation and, if necessary, to change their legislation to meet the EU's standards[14].

3.2 APEC Privacy Framework

The Asia Pacific Economic Cooperation (APEC) developed the APEC Privacy Framework, which was finalized in 2005. The Framework is largely consistent with the OECD Guidelines of 1980, and aims to improve the standard of information privacy protection throughout the APEC member economies and to increase the trans-border flow of personal information between these countries[10]. The framework is composed of two parts: Part A lays out nine Data Protection principles to promote domestic implementation of privacy protection standards in APEC member countries; Part B addresses the cross-border implementation of the principles through the Cross-border Privacy Rules(CBRPs)[7].

At its essence, the Framework recognizes the need to eliminate disparities between the national laws of APEC member countries so that the free flow of information across borders is not unduly hampered while maintaining a minimum level of protection[10]. However, the underlying characteristic of APEC as a loose-knit economic cooperation mechanism which, unlike EU, on principle respects the different approaches taken by each member economy, remains predominant[10]. Consequently, the Framework does not have meaningful enforcement requirements and therefore, serves no more than a policy recommendation or guideline, the application of which is largely voluntary[7].

Accordingly, the extent of development of personal data and privacy protection standards across the Asia-Pacific remains diverse, despite the endorsement of the APEC Privacy Framework[10]. By and large, the APEC Framework is an example of setting a minimum standard – a floor rather than a ceiling – of personal data protection at a regional level with a practical aim to ensure the compatibility of national laws and thereby facilitate regional economic cooperation[7]. In contrast to the strong political institution which underpins a universal, harmonized enforcement mechanism to take root in the EU, the political implication of APEC data protection framework remains largely insignificant.

3.3 Sectoral Approach of the United States

In the United States, the right to privacy can be traced to the United States Constitution and to common law[14]. In the Constitution, which is one of the most influential American articles on the right to privacy, it is argued that privacy was "*the right to be left alone*"[14]. Since then, the United States Supreme Court has stated that the Constitution protects "the individual interest in avoiding disclosure of personal matters" and "the interest in independence in making certain kinds of important decisions"[17]. However, the Court has also held that the right to privacy was not absolute and an individual's privacy interest must be balanced against "competing public interests"[17].

Reflecting the legal tradition, the right to privacy in

the United States, unlike the European approach, protects only against the federal government's infringement into an individual's privacy[14]. Therefore, the legislation specific to the issue of personal data protection is limited to data processed by and in use of the federal government[13]. Other than a few laws dealing with personal financial and medical information, the United States does not have legislation or exercise enforceable standards that govern the processing of personal data by private organizations[17]. Instead, the U.S. system provides self-regulation by industry of the personal data handled by private organizations[14]. Therefore, industries in the United States are mostly self-regulated. In this sense, the U.S. approach does not necessarily support the concept of establishing an enforceable standard on global personal data protection over the Internet, which goes beyond the scope of trade facilitation and touches the issue of privacy as a fundamental human right. Such an understanding is also testified by the U.S. Federal Trade Commission(FTC) and Department of Commerce, as they have made clear the goal to ensure that "*the growing, changing, thriving information marketplace is built on a framework that promotes privacy, transparency, business innovation, and consumer choice*"[8].

In terms of the trans-border transfer of personal data, the FTC has developed the Safe Harbor Framework through which an organization receives a certification assuring that it provides an adequate level of protection to personal data[8]. Although this provision is voluntary in the domestic context, companies that receive personal data from members of the EU should adopt these guidelines for the cross-border handling of information. The Safe Harbor Framework was proposed by the U.S. Department of Commerce and subsequently approved by the EU in 2000 with an aim to ensure safe passage of data from Europe to the United States[8]. As noted previously, such a framework was largely necessary due to the different approaches taken by the EU and the US in trans-border data protection. It is worth mentioning that the U.S private companies who signed up to the Safe Harbor list would adhere to the rules set out by the EU, while the U.S. law and standards would not change. For example, for a European citizen who uses Gmail provided by the U.S-based Google, the Safe Harbor Framework ensures an EU-level data protection standard, rather than that of U.S. laws.

In a sense, the measure somehow represents a cross-regional effort to address international transfer of personal data and prevent any conflicts that may arise from the lack of international standard. However, it is limited in two ways. First, the Framework is a voluntary, self-regulated measure by the private sector as opposed to being directly regulated by the U.S. government, and therefore falls short of adequate level of enforceability in its political implication. Second, since it primarily concerns trade facilitation between the EU and US rather than driven by the principle of universal rights to privacy, personal data may be liable for inspection in many exceptional cases, for example, by the U.S. authority under the US Patriot Act[8].

3.4 A Transition from Sectoral to Comprehensive National Approach: South Korea

In South Korea, the data protection law was first introduced with the Public Agency Data Protection Act of 1995 to cover the practice of its public sector[8]. For the personal data handling of the private sector, the practices were largely sectoral until the Act on Promotion of Information and Communications Network Utilization and Information Protection of 2001 was enacted to be applied most generally to entities that process personal data for profit through telecommunication networks and computers. The 2001 Act was influenced strongly by the OECD Guidelines, and was eventually strengthened in 2004 beyond the criteria set forth by the OECD, notably on matters such as data breaches and data exports[8].

In 2011, a new Personal Information Protection

Act(PIPA) was passed . This new act is worth a closer investigation considering its comprehensiveness of application and a higher level of standard required for both public and private actors – a major transition from the U.S. driven sectoral approach examined earlier. One of the most important changes in the new Act was that all data processors, both public and private, came under the subject of a single act, the PIPA, which completely replaced the previous public sector Act[7]. In addition, manually processed information has become a subject of the same protection as is the case for automatically processed data. An independent Data Protection Commission (DPC) under the Presidential Office, composed of 15 members (including a chairperson and a standing commissioner) deliberates on policy issues, laws and regulations and standards, and investigates breaches of the Act and refers matters for prosecution[8]. Moreover, other new mechanisms for dispute resolution are added. Collection and use of sensitive data, including universal identifiers like the resident registration number, are prohibited without the specific consent of data subjects or authorization by law[8].

In terms of the trans-border transfer of personal data, PIPA provides specific statements. It mentions "*When the personal information processor provides personal information to a third party overseas, it shall inform data subjects (…), and obtain consent from 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*"[8].

Overall, Korean data protection standards are generally considered as exceeding the OECD standards and one of the strongest in Asia. For example, the Japanese counterpart, the Personal Information Protection Act of 2003 adopts a self-regulatory approach to manage privacy issues in the public sector[16]. Furthermore, companies that hold personal data of 5,000 people or less and ordinary private use of personal information are exempt from the requirements of the standard[16]. With regard to the trans-border transfer, there is no separate restriction on the trans-border transfers of personal data from Japan to a third country, though there is a general restriction on transfers to third parties.

Coupled with the overall shift from a sectoral to a more expansive legislation for personal data protection, the Korean government has started efforts to strengthen its influence in the international community, where the EU and the U.S. currently dominate the discussion.

As a recent example, in November 2012, the Korea Communications Commission(KCC) announced that the Korean national standard of Personal Information Management System(PIMS) was adopted as a new topic at the joint technology committee of International Standard Association(ISO)/International Electrotechnical Commission(IEC) for the first time. PIMS was started in 2011 as a Korean national standard to guide companies to protect the personal data of their customers in a systematic and sustainable manner. As the topic has received recognition from the joint committee of the two most significant authorities in the global standardization arena, Korea is expected to position itself as one of the leaders in personal data and privacy protection in the world.

As the KCC noted, if the PIMS succeeds to become an international standard, its influence to the resolution of potential trans-border data transfer disputes would be significant in international trade, particularly amid the growing number of Free Trade Agreement(FTA) negotiations. Moreover, the expansion of PIMS as a recognized international standard would bring another economic benefit to Korean businesses, as the size of global standard and certification market for Korean certification agencies would eventually increase encompassing developing countries where the related laws and standards on data and privacy protection are relatively weak.

In comparison to the EU strategy of internationalizing its strict data protection principle through mandatory regulations, the initiative of the

Korean government for international standardization has its merits in terms of promoting a successful domestic standard on personal data protection to global stakeholders.

4. Discussion

4.1 Where we stand: At the two extremes of a spectrum

As reviewed in the two regional cases of EU and APEC, and the two national ones of U.S. and Korea, many states and regional organizations have forged divergent laws and standards on data protection that are not compatible and in some cases, even confront each other.

Currently, the discussions are largely dominated by two powerhouses: the European Union(EU), representing the hardline human rights perspective on one end; and multinational ICT companies, many of them based in the United States such as Google and Facebook on the other extreme, which support self-regulatory principles typified by minimum government regulation and maximum economic efficiency. Surrounding the two extreme cores on the spectrum, other states and regional entities gather around with different degrees of emphasis.

For example, a large room for flexibility found in the APEC guidelines provides a glimpse of where privacy principles are headed in this regional organization – which comes closer to a sectoral, self-regulatory regime of the U.S. The case of Korea is an interesting example which represents a shift of the privacy governing principle from a sectoral to a more comprehensive means, which, to a certain extent, resembles the EU-style strong enforcement.

In the recent dispute between the EU Data Protection Directive and the Facebook regarding the arguably privacy-infringing nature of the American firm's new face recognition tool, the increasing tension has sparked discussions in the international political arena. Advocates of a strong, enforceable global mechanism call that the impending proposals to revise the EU Data Protection Directive should serve as a cornerstone to set up a form of international convention to strengthen individual rights[5]; while others, including the Facebook, openly try to garner support from the public that such a measure is simply unreasonable and unrealistic[15].

The discussion to find a solution to the current discrepancy should first start by understanding that the challenges related to the personal data protection standards are primarily societal in nature.

For example, the definitions and the scope of national legislative approaches differ significantly from country to country. How do states define personal data and right to privacy? Who are the main stakeholders when developing a socially agreed-upon definition of personal data protection and privacy? During that process, who participates, i.e. the government, private sector, civil society? Do national legislations apply to both public and private entities? These questions, along with the different answers to them, reflect that data protection mechanism is inherently an issue of the societal agreement in a given context.

In addition, it is important to understand that political challenges inherently arise in regional, global efforts to develop and implement a data protection mechanism to ensure compatibility and compliance. Obviously, considering the increasing volume of trans-border flow of personal information, achieving coherency in privacy protection within regional and/or global communities is important. However, there is also a need to take into account the differences in contexts.

Notably, the EU Data Protection Directive has a legal and institutional authority to individual EU member states, which is supported and reinforced by the strong level of political, economic and social integration within the regional bloc. As such, the Directive has its specific aim which is to raise the bar for privacy and data protection between the European and non-European states, along with practical

measures, at least within the region, to draw out political cooperation[18].

There are other examples of political negotiation found between state and regional actors. For example, the adoption of the Safe Harbor Framework ensures that the EU-level protection is guaranteed in the U.S. However, there is also a potential clash surfacing on the ground between the enforcing agencies in the EU and the multinational companies based in the U.S. As mentioned earlier, on the other hand, the EU Commission recognized that New Zealand's data protection standards are fully competible to those of EU.

By and large, the key issue surrounding the personal data protection over the Internet dwells in how to ensure globally compatible, enforceable measures to be put in place in a social and political sense, which goes further than merely raising mutual understanding of the importance of the topic. Beyond the discussion of idealism from both ends of the spectrum, what type of international framework would, or should emerge in a practical sense, taking into account of the sociopolitical challenges?

4.2 Idealism and Realism: Towards a practical solution to data protection

Undoubtedly, there are several ongoing efforts to set up a globally applicable solution to the data and privacy protection issues.

First, the possibility of multilateral conventions can be considered as one of the strongest measures to provide a legally binding, universal protection of privacy rights. The idea has been considered as a somewhat natural solution for those advocates of individual rights, stemming from the ideals of the UN Declaration of Human Rights. Bygrave, for example, envisaged a form of international treaty to be drafted by the International Law Commission(ILC) and adopted by states through the United Nations[2]. Greenleaf, on the other hand, mentioned that the current EU Convention 108, stands as a promising candidate for a global instrument to govern online privacy[9]. Indeed, as COE considers 'globalizing' its Convention 108 through revisions and spells out the desirable standard of data protection and privacy at a global level, such a comprehensive legal framework in the form of an international convention seems to gain weight.

However, such a measure is unlikely to bear fruit unless states decide to make it become a binding international law. As Greenleaf notes, global conventions often take decades to obtain a 'critical mass' of ratification[9]. In order to reach a threshold of the critical mass, should the requirements be set at the minimum level to ensure participation of as many state actors as possible, or be aimed at the maximum level to uphold the symbolic significance of an international convention at the cost of the scope of participation? Again, it reveals the challenge of striking a right sociopolitical balance among states and regional actors, in addition to the sheer amount and intensity of discussions to bring about individual state's commitment and to reach a consensus. In this sense, the ideal of a universal protection of individual privacy rights seems not quite practical at the moment.

Regional conventions and treaties can be considered. Compared to the global level convention, it has an advantage that a regional, supranational organization such as the EU may directly adopt texts that have the force of law in all member states. Notably, a growing number of countries now enact data privacy laws covering their public and private sectors. This recent change that is increasingly observed even outside of the Europe exhibits that national governments have started recognizing the importance of data protection.

However, as seen in the case of APEC Framework, the enforceability issue arises when the umbrella regional organization does not have constitutions which make the adoption of the Framework mandatory to its member states. With this reason, the APEC Framework is considered a model law that can only assist state governments in preparation of national legislation. Similar to the case of a global convention,

the following process under a politically loose-knit regional entity will take a lot of determined work to achieve a communal agreement.

Obviously, as Bennett points out, there is a common resistance to data protection law by those who regard it as an unnecessary intervention to a problem that should be treated with a combination of self-regulation and litigation[1]. Notably by the U.S. business, the European Data protection measures are considered an unjust attempt to transplant data protection regulation to another country where the constitutional system and political cultures are very different[1]. In this sense, the legal, normative attempt at establishing an international convention on data protection is not likely to take effect. At the same time, however, it should be observed that other commentators criticize the fragmented, incoherent and often reactive manner in which the U.S. driven privacy protection approach, under the ideal of laissez-faire principle, has been formed[1]. Such a process has resulted into a variety of voluntary, sectoral codes of conducts on data protection, which are considered largely insufficient to proactively and preventively address the myriad of issues concerning the increasing flow of trans-border data transfer. In sum, the situation requires a breakthrough to enter a discussion for a more practical solution, a shift of the principle from idealism to realism.

4.3 International Standardization of Data Protection and Privacy

Against this backdrop, a more realistic solution to the current tension between the two ideals might lie in establishing an internationally recognized technical or policy standard on data protection. Compared to the other two solutions – a multilateral convention and sectoral codes of conducts postulated by the two camps respectively –, an international standard has its merit in potentially certifying the practices and policies and thus giving a “good housekeeping seal of approval”[1]. Particularly, the case of Korea, which recently jumped on the wagon notably by joining the standardization process of privacy protection framework at the ISO, presents a snapshot of the turnaround.

A standard by definition is a voluntary instrument, which is developed through a voluntary cooperation among industry, consumers, public authorities and other interested parties[3]. However, despite the voluntary nature, standards have already formed an important privacy-protection measure in many domains[18]. Notably, through an established consensus-building process, some aspects of privacy as a multifaceted concept have been defined at the ISO and thereby officially accepted at the international level. For example, the ISO/IEC Joint Technical Committee SC 27 was established in 1989 to address the issue of IT security techniques. Currently, it has embarked on the task of standardizing the Privacy Framework to protect individual privacy right.

Obviously, a separate ISO privacy standard would carry a significant weight and credibility to individual states. For example, it would also attract attention from different national standard bodies to participate in the international effort to certify what is expected in the data protection protocol. In addition, it would give, particularly to the business, a strong incentive to demonstrate their conformity to international data protection standards.

This issue of providing an incentive for compliance has been largely neglected in the legal and regulatory approaches to the international data protection framework. International standards provide a reliable mechanism for the implementation of trans-border regulations. For example, required registration to a standard, which would oblige independent and regular auditing, would provide a greater certainty that an “adequate” level of data protection is being practiced by the receiving end - those non-EU states under the case of the EU framework - regardless of its location[1]. Even though the process of international standardization requires accompanying efforts to harmonize systems of conformity assessment and

auditor certification[1], the existing institutional foundation of international standard organizations notably including the ISO can greatly strengthen the incentive for adoption and compliance while lowering the societal cost of harmonization at a global level.

Another advantage of an international standard includes the sociopolitical balance it tries to achieve through the process of cooperation. As noted, the defining factor that sets apart idealism and realism of the global data protection regime is whether an agreed-upon solution could emerge from political and societal negotiation. In this light, the existing institution of international standardization may serve as a proven, neutral ground upon which stakeholders including the states and multinational ICT companies can search for, and agree on, a common solution under the label of an international standard.

Unlike the existing voluntary codes of conducts promoted by the self-regulatory approach, the "adoption" of the standard means somewhat political, which is more than a symbolic claim but a claim verified by the regular and independent auditing of policies and practices drawn from the institution of a globally recognized standardization mechanism[1]. In this light, as Bennett states, in the absence, and the impracticality of international law, "*international standard can operate as a commonly accepted yardstick of good privacy practice and a ready-made model for any business, government and other stakeholders*"[1].

5. Conclusion

The progress made in ICT – which has brought tremendous social and economic benefits – makes the processing and exchange of data across international borders relatively easy and often necessary. The challenge, therefore, is to protect fundamental rights and freedoms, notably the right to privacy and the right to personal information, while encouraging the free and secure flow of information within and across borders, which is essential to the continued expansion of cloud computing, and other web-based services. As reviewed, the approaches taken by the EU and the U.S. respectively are dominating the international discussion, but it is unlikely that a solution that is ideal for one side is also ideal for another.

In sum, the key to establishing a functioning international solution for personal data protection lies in striking a right balance between the two camps which currently dominate the discussion – the advocates of individual privacy rights on one side, and the proponents of self-regulation and economic efficiency on the other. In the face of a growing tension between the two sides each equipped with their own ideals, a practical solution may lie in utilizing established institutions of standardization as a ground upon which an agreement can take its root.

참 고 문 헌

[1] Bennett, C.J. (1997). Arguments for the Standardization of Privacy Protection Policy: Canadian initiatives and American and international responses. *Government Information Quarterly*, 14(4), pp.352-364.

[2] Bygrave, L.A. (1998). Data Protection Pursuant to the Right to Privacy in Human Rights Treaties. *International Journal of Law and Information Technology*, 6, pp.247-284.

[3] Commission of the European Communities (2009). White Paper: Modernising ICT Standardization in the EU – The Way Forward. EU, Brussels.

[4] Dumortier, J. & Goemans, C. (2000) Data Privacy and Standardization. Brussels.

[5] European Commission (2012). Commission to Renegotiate Council of Europe Data Protection Convention on Behalf of EU. Brussels.

[6] European Commission (2012). EU Approves New Zealand's Data Protection Standards in Step to Boost Trade, Brussels: EU.

[7] Greenleaf, G. (2009). Five Years of the APEC Privacy Framework: Failure or promise. *Computer Law and Security Review,* 25, pp.28-43.
[8] Greenleaf, G. (2011). Major Changes in Asia Pacific Data Privacy Laws: 2011 Survey. *Privacy Laws & Business International Report*, pp.5-14.
[9] Greenleaf, G. (2012). The influence of European Data Privacy Standards Outside Europe: Implications for Globalisation of Convention 108?. University of Edinburgh, Edinburgh.
[10] Kennedy, G., Doyle, S., Lui, B. & Contributors (2009). Data Protection in the Asia-Pacific Region, *Computer Law and Security Review*, 25, pp.59-68.
[11] Kenyon, A.T. & Richardson, M. (2006). New Dimensions in Privacy Law: International and Comparative Perspectives, Cambridge, UK: Cambridge University Press.
[12] Kuner, C. (2009). An International Legal Framework for Data Protection: Issues and Prospects. *Computer Law and Security Review*, 25, pp.307-317.
[13] Kuner, C. (2010). Data Protection Law and International Jurisdiction on the Internet (part 1). *International Journal of Law and Information Technology*, 18(2), pp.176-193.
[14] OAS (2011). Preliminary Principles and Recommendations on Data Protection. Organization of American States, Committee on Juridical and Political Affairs.
[15] Ramasastry, A. (2012). The Right to Be Untagged: As Facebook Disables Facial Recognition for EU Consumers, U.S; Consumers Are Left Wondering What's Next for Them, Justia News.
[16] Rohlmeier, J. (2011). International Data Protection Legislation Matrix. U.S. Department of Commerce.
[17] Stratford, J. S. & Stratford, J. (1998). Data Protection and Privacy in the United States and Europe. *IASSIST Quarterly*, 19, pp.17-20.
[18] Wright, D., Gutwirth, S., Friedewald, M., De Hert, P., Langheinrich, M. & Moscibroda, A. (2009). Privacy, Trust, Policy-Making: Challenges and Responses. Computer Law & Security Review, 25, 69-83.
[19] http://www.un.org/en/documents/udhr/index.shtml
[20] http://assembly.coe.int/Main.asp?link=/Documents/WorkingDocs/Doc11/EDOC12695.htm
[21] http://www.coe.int/t/dghl/standardsetting/dataprotection/convention_en.asp
[22] http://www.oecd.org/internet/interneteconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm
[23] http://www.oecd-ilibrary.org/docserver/download/5kgdpm9wg9xs.pdf?expires=1355367608&id=id&accname=guest&checksum=786B17CA249B25B7915BB8F0871523BA
[24] http://www.un.org/documents/ga/res/45/a45r095.htm
[25] http://www2.ohchr.org/english/law/ccpr.htm

주 한 나

・2003년 2월 : 연세대학교 교육학과 (교육학·사회학사)
・2007년 5월 : New York University 공공행정대학원(석사)
・2011년 9월 ~ 현재 : 연세대학교 국제학대학원(박사과정)
・관심분야 : 정보통신표준
・E-Mail : hanah.zoo@yonsei.ac.kr

이 희 진

・1986년 2월 : 서울대학교 경영학과 (경영학사)
・1989년 2월 : 서울대학교 사회학과 (석사)
・1997년 8월 : London School of Economics 정보시스템(박사)
・1998년 8월~ 2002년 6월 : 영국 Brunel대학교 교수
・2002년 7월 ~ 2006년 2월 : 호주 멜번대학교 교수
・2007년 3월 ~ 현재 : 연세대학교 국제학대학원 교수
・관심분야 : 중국의 정보통신표준
・E-Mail : heejinmelb@yonsei.ac.kr

곽 주 영

- 1998년 2월 : 서울대학교 중어중문학과(문학사)
- 2000년 8월 : 서울대학교 경제학과(석사)
- 2008년 8월 : Massachusetts Institute of Technology(Ph.D. in Technology Economics and Policy)
- 2008년 8월 ~ 2009년 8월 : Massachusetts Institute of Technology, Research Fellow
- 2009년 9월 ~ 현재: 연세대학교 경영대학 교수
- 관심분야 : 글로벌 전략적 제휴, 개발도상국(특히 중국 및 화교경제권), 기업 간 네트워크
- E-Mail : jooyoung.kwak@yonsei.ac.kr

김 용 영

- 1996년 2월 : 충북대학교 경영학과(경영학사)
- 1999년 2월 : 서울대학교 대학원 경영학과(경영학석사)
- 2007년 2월 : 서울대학교 대학원 경영학과(경영학박사)
- 2011년 3월 ~ 현재 : 건국대학교 경영경제학부 조교수
- 관심분야 : 정보보호, 프라이버시, 정보기술 수용 전후 사용자 행태, 모바일 및 스마트 비즈니스
- E-Mail : kyyoung@kku.ac.kr