PRIVACY AND SECURITY PROTECTION UNDER KOREAN E-COMMERCE LAW AND PROPOSALS FOR ITS IMPROVEMENTS*

Kyung Han Sohn**

TABLE OF CONTENTS

I. INTRODUCTION

Daum–Kakao Corporation (Kakao) is the largest social network service (SNS) company in Korea.[1] In early October 2014, Korean netizens, or citizens of

* This paper was presented at the Second Pacific Rim Colloquium held on January 9, 2015, in Shanghai, China. The author wishes to express his deep gratitude for the

the Internet, suddenly transferred their use of SNS from Kakao to Telegram, a SNS from Germany.[2] This sudden transfer of users occurred as soon as Kakao revealed that it had complied with warrants from Korean investigation agencies that were conducting surveillance on its Kakao users' communications.[3] Newspapers named the incident the "Cyber Asylum from Korea."[4] On October 14, 2014, Kakao declared that it would no longer accept surveillance writs but rather will subject itself to criminal sanctions from the Korean government.[5] Furthermore, the company introduced a private SNS in which no one could intervene.[6] This incident demonstrated the sensitivity of the Korean netizens on privacy issues over security concerns.

The Korean legal environment promoting privacy and security protection in E-commerce has evolved over the last 20 years through the passage of the 1999 Electronic Transaction Framework Act (E-Documents Act)[7] along with the E-Commerce Consumer Protection Act (ECCPA) for privacy[8] and the Electronic Financial Transaction Act (EFTA) for security.[9] In addition, several statutes have

---

invitation to the colloquium by Professor Boris Kozolchyk and other organizers of the colloquium.

** Professor at Sungkyunkwan University School of Law & Senior Member of Jung & Sohn, Seoul, Korea (admitted to the Korean & New York State Bars).

1 *Kakao Story is Top Social Media in Korea: Survey*, KOREA HERALD TIMES (Apr. 14, 2015, 3:15 PM), http://www.koreaherald.com/view.php?ud=20150414000867.

2 *Threat of Government Surveillance has KakaoTalk Losing Users to German-Based App*, KOREA TIMES US (Oct. 8, 2014), http://www.koreatimesus.com/threat-of-government-surveillance-has-kakao-talk-losing-users-to-german-based-telegram/.

3 Kim Jae-seok, *Kakao Worried About Government Agencies Response After Info Release*, HANKYOREH (Oct. 10, 2014, 11:22 AM), http://www.hani.co.kr/arti/english_edition/e_national/659194.html (noting that Daum and Kakao received 147 warrants from intelligence investigative authorities, including the National Intelligence Service (NIS), prosecutors, police, and the Korea Communication Commission (KCC)).

4 *KakaoTalk on Notice: Telegram Targets Korean Market Utilizing Popularity with Cyber Asylum Seekers*, BUSINESS KOREA (Oct. 9, 2014, 11:40 PM), http://www.businesskorea.co.kr/article/6703/kakaotalk-notice-telegram-targets-korean-market-utilizing-popularity-cyber-asylum.

5 Song Jung-a, *Koreans Lose Faith in Homegrown Chat Apps*, FINANCIAL TIMES (Oct. 16, 2015, 12:43 PM), http://www.ft.com/intl/cms/s/0/fb00386a-5440-11e4-84c6-00144feab7de.html#axzz3mcI4xpDE.

6 *Id.* The company also planned to reduce the length of time messages are stored on its servers and introduce encryption features on the messaging application. *Id.*

7 *See generally* Framework Act on Electronic Documents and Transactions, Act No. 5834, Feb. 8, 1999 (S. Kor.), *translated in* Korean Legislation Research Institute online database, http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=5054&type=part&key=28 [hereinafter E-Documents Act].

8 *See generally* Act on the Consumer Protection in Electronic Commerce, Etc., Act No. 6687, Mar. 30, 2002, *amended by* Act No. 11461, Jun. 1, 2012 (S. Kor.), *translated in* Korean Legislation Research Institute online database, http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq=25650&type=new&key= [hereinafter ECCPA].

9 *See generally* Electronic Financial Transactions Act, Act No. 7929, Apr. 28,

enhanced the protection of privacy and security within the Internet community, including the E-commerce market. However, the Korean system for privacy and security protection has many shortcomings and hinders the development of E-commerce.

This paper proposes potential steps for improving Korean privacy law and security law related to E-commerce after comparing the current status in Korea to relevant U.S. and European Union (EU) laws. These improvements would contribute to the development of global uniform E-commerce rules for additional privacy and security protections on an international scale.

II. AN OVERVIEW OF E-COMMERCE LAW IN KOREA

In order to understand the privacy and security laws related to E-commerce in Korea, it is necessary to have an overview of Korea's complex system of E-commerce regulation. This section provides an overview of the various pieces of legislation that have been adopted in Korea over the past 20 years in order to improve regulation of E-commerce.

A. Legislative Developments

The first step in developing the legal system promoting E-commerce was the enactment of the E-Documents Act[10] and the Digital Signature Act (DSA) in 1999.[11] Once the United Nations Commission on International Trade (UNCITRAL) announced its Model Law on Electronic Signatures in 2001,[12] the Korean government amended the DSA in 2002.[13] In order to protect consumers in E-commerce, the ECCPA was enacted in the same year.[14] The need for safety in financial transactions led to the introduction of the EFTA in 2006. These legislative efforts demonstrate the Korean government's commitment to establishing sophisticated regulations on E-commerce since 1999, and this commitment has evolved continuously.

2006, *amended by* Act No. 11461, Jun. 1, 2012(S. Kor.), *translated in* Korean Legislation Research Institute online database, http://elaw.klri.re.kr/eng_service/lawView.do?hseq=30515&lang=ENG [hereinafter EFTA].

[10] *See* E-Documents Act, *supra* note 7.

[11] *See* Digital Signature Act, Act No. 5792, Feb. 5, 1999, *amended by* Act No. 11690, Mar. 23, 2013 (S. Kor.), *translated in* Korean Legislation Research Institute online database, http://elaw.klri.re.kr/eng_service/lawView.do?hseq=28791&lang=ENG [hereinafter DSA].

[12] *See* G.A. Res. 56/80 (July 5, 2001) [hereinafter 2001 UNCITRAL Model Law on Electronic Signatures].

[13] *See supra* note 11.

[14] *See* Electronic Communication Privacy Act, 18 U.S.C. § 2510 (1986) [hereinafter ECPA].

B. Framework Act on Electronic Documents and Transactions

As mentioned above, the E-Documents Act provided the first basic E-document and E-transaction regulation when it was introduced in 1999, accompanied by the DSA.[15] The E-Documents Act is modeled after the Model Law on Electronic Commerce, which was promulgated by UNCITRAL in 1996.[16] The E-Documents Act for the first time recognized an electronic record as a legal document.[17] Namely, neither the legal validity nor the qualification of an electronic document as evidence would now be denied.[18] Furthermore, the E-Documents Act recognized the legal validity of a certified digital signature.[19]

The E-Documents Act specified the time and place of transmission or the receipt of electronic documents. For the safety of consumers participating in E-commerce transactions, the E-Documents Act designed the establishment of accredited certification authorities.[20] Furthermore, the E-Documents Act introduced a mechanism for resolving E-commerce disputes caused by, *inter alia,* infringement of privacy and security.[21] Under the E-Documents Act, the Electronic Commerce Mediation Committee (ECMC) was formed in 2000.[22]

The Korean legislature has amended the E-Documents Act to improve the E-Commerce legal framework five times: in 2002,[23] 2005,[24] 2007,[25] 2008,[26] and 2012.[27] The 2002 Amendment provided that an electronic document is

---

15 *See supra* notes 9-11 and accompanying text.

16 *See* G.A. Res. 51/162 (June 12, 1996) [hereinafter 1996 UNCITRAL Model Law on Electronic Commerce].

17 E-Documents Act, *supra* note 7, art. 7. The current version of the ETFA further clarifies the legal validity of electronic documents. *Id.* art. 4, § 1 ("No electronic document shall be denied legal effect as a document solely because it is in an electronic form, except as otherwise expressly provided for in other Acts.").

18 *Id.* art. 7 ("An electronic message shall not be denied its evidential weight in litigation or any other legal proceedings on grounds that it is in the electronic form.").

19 *Id.* art. 6, § 1.A "digital signature" within the meaning of the ETFA means "a signature in a kind of electronic form which represents the identity of any originator of an electronic message, and the fact that the electronic message is generated by the originator." *Id.* art. 2, § 4.

20 Certified digital signatures were issued by government-authorized certification authorities in accordance with Articles 16 and 17 of the ETFA. E-Documents Act, *supra* note 7, arts. 16-17.

21 *Id.* art. 28 ("The government shall prepare policy measures necessary for the establishment and operation of the dispute settlement body and the settlement of disputes arising from electronic commerce in order to remedy damages resulting from improper electronic trading and to establish optimum electronic commerce practices.).

22 Kyung-Han Sohn, *Alternative Dispute Resolution System in Korea*, SOFTIC SYMPOSIUM (2002), http://www.softic.or.jp/symposium/open_materials/11th/en/Sohn.pdf.

23 E-Documents Act, *supra* note 7, Act No. 6614 (2002).

24 *See id.* at Act No. 7796 (2005).

25 *See id.* at Act Nos. 8362, 8371, 8387, 8461, 8466, 8802 (2007).

26 *See id.* at Act Nos. 8852, 8932, 8979, 9246 (2008).

27 *See id.* at Act No. 11461 (2012).

deemed to be sent from or received at the habitual residence of the originator or addressee if he or she does not have a place of business.[28] It also included improvements in consumer protection such as the Certified E-Merchant System.[29] Additionally, it imposed a duty on the government to set up E-commerce policies.[30] Government procurement of E-commerce is expanded under the amendment due to its command to set up additional policies.[31]

The 2005 Amendment to the E-Documents Act established Certified Electronic Commerce Support Centers (ECSC).[32] ECSCs are required to store electronic documents safely and accurately. Each ECSC must issue a certificate when it provides storage services.[33] The certificate has information regarding the contents; the originator; the recipient; and the date and time of storage of, the transmission of, and the receipt of the electronic documents stored.[34] This information is presumed to be true.[35] Additionally, the legislation listed the statutes that provide for when an electronic document is as legally valid as a paper document.[36]

Amendments to the E-Documents Act in 2007 and 2008 led to the replacement of the storage of paper documents by the storage of electronic documents, as the amendments provided for stricter regulation on AEDCs including transfer of AEDC business.[37] They set forth the E-commerce operators' liability for compensation and duty to insure.[38] They also strengthened consumer protection by granting consumers the right to withdraw offers, cancel or terminate contracts, or return goods.[39]

In 2012, the E-Documents Act was renamed to the Framework Act on Electronic Documents and Transactions (FAEDT).[40] Also, the new law

---

[28] E-Documents Act, *supra* note 7, at Act No. 6614, art.6 § 3 (2002).

[29] *Id.* art. 18.

[30] *Id.* art. 12-16, § 1 (2002) (enabling the Korean government to formulate policies to further the protection of personal data, business secrets, and general consumer interests, while also giving the government power to create policies directed at preventing damages or other negative effects of E-commerce transactions).

[31] *See, e.g.*, *id.* art. 19 ("The Government shall, for the promotion of electronic commerce, formulate and execute the basic policy on electronic commerce pursuant to the principles, such as the promotion under private initiatives, minimization of regulations, security for the safety and reliability of electronic commerce, solidification of international cooperation.").

[32] *Id.* at Act No. 7796, art. 31-2, § 1-2 (2005).

[33] E-Documents Act, *supra* note 7, Act No. 7796, art. 31-2 § 1-2 (2005).

[34] *Id.* art. 31-7, § 2.

[35] *Id.*

[36] *Id.* art. 4, § 2, add. (2005).

[37] *Id.* at Act No. 9246, arts.31-1 to 31-16 (2008).

[38] E-Documents Act, *supra* note 7, Act No. 9246, art. 31-16, § 1-2 (2008).

[39] *Id.* art. 17.

[40] Electronic Document & Electronic Transaction Framework Act, Statutes of the Republic of Korea, Act. No. 11461, art. 1, 2012 (S. Kor.), *translated in* Korean Legislation Research Institute online database, http://elaw.klri.re.kr/eng_mobile/viewer.do?hseq

introduced the Certified E-mail Address (CEA) system and the Authorized Electronic Document Intermediary (AEDI).[41] CEAs can be registered at the National Information Technology Industry Promotion Agency (NIPA).[42] NIPA stores the date and time of transmission and reception of electronic messages and transactions via the CEAs.[43] NIPA issues a certificate of transmission to the party concerned.[44] The amendments strengthened regulation of Internet advertisements and prohibited the transmission of advertisements by CEAs for profit.[45] The amendment set up penal sanctions to ensure the reliability of electronic document distribution.[46] The 2012 FAEDT prohibited the wrongful use of a Certification Mark for Best E-Merchant.[47] It also made settlements entered into at the ECMC immediately enforceable without a court judgment.[48]

In relation to international treaties regarding E-commerce regulations, Korea signed the 2006 United Nations Convention on the Use of Electronic Communications in International Contracts (E-Contract Convention).[49] The Korean government tried to introduce the content of the E-Contract Convention in the 2012 amendment to the E-Documents Act.[50] The effort failed due to disagreement among governmental ministries.[51] The Korean government had not yet ratified the E-Contract Convention as of 2015.

C. Digital Signature Act

The DSA was enacted in 1999 to establish a basic framework for regulating electronic signatures in a legislative effort to ensure the integrity and reliability of electronic messages.[52] Although the DSA did not specifically adopt encryption technology, it gave the government the power to do so, and the Public

---

=27334&type=part&key=28 [hereinafter FAEDT].

[41] CEA means an address registered pursuant to the ETFA, which is comprised of letters and numbers to identify a person who sends or receives an electronic document and AEDI means a person designated under the ETFA, who provides the service of storage of electronic documents for others. *See* E-Documents Act, *supra* note 7.

[42] *Id.* at Act No. 11461, art. 18-4 (2012).

[43] *Id.* art. 18-5, §1.

[44] *Id.* art.18-5, §2.

[45] *Id.* art. 18-7.

[46] *See* E-Documents Act, *supra* note 7, at Act No. 11461, art. 31-5 (2012).

[47] *Id.* arts. 18-2, 46 §2(1).

[48] *Id.* art. 35, §3 ("A protocol of mediation . . . shall have the same effect as a consent judgment under the Civil Procedure Act.").

[49] *See* U.N. Convention on the Use of Electronic Comms. in Int'l Contracts, U.N. Doc. A/C.6/60/L.8 (Jan. 24, 2006) [hereinafter E-Contract Convention].

[50] Wan-Yong Chung, *A Study on the Proposal for the Revision of the Framework Act of the Electronic Documents and Electronic Commerce*, 48 KYUNG HEE U. L. REV. 631, 632-71 (2013).

[51] *Id.* at 633.

[52] *See generally* DSA, *supra* note 11, at Act No. 5792(1999).

Key Infrastructure (PKI) system of encryption technology was adopted as a result.[53] Under the DSA, digital signatures are classified into either the Certified Digital Signature or the General Digital Signature.[54] The DSA first covered the issue of Licensed Certification Authorities (CA), and it marked the beginning of the license system of Accredited CAs.[55] Under the DSA, a digital signature created by a private key corresponding to a public key listed in the certificate issued by the Accredited CAs is deemed a legally effective signature or signature-seal.[56] The DSA provides that digital signatures are presumed to be the signature of the person "signing" the document.[57] Further, the DSA presumes that such documents are unaltered after they are digitally signed.[58] Also, the DSA provides security and reliability of certification practices, including the requirements for issuance and revocation of a certificate and for the Digital Signature Certification Policy to be established by CAs.[59]

An amendment to the DSA in 2002 followed the 2001 UNCITRAL Model Law on Electronic Signature.[60] By allowing the government to establish whatever encryption technology they determined most effective, the DSA adopted technological neutrality instead of the PKI or asymmetry cryptography methods.[61] In 2006, the DSA was further amended to divide the certification work among CAs.[62] The 2006 Amendment created digital signature certification work guidelines and imposed a duty on CAs to establish rules of certification work.[63] The Amendment was aimed at ensuring greater protection for the users and went as far as including an imposition of a legal duty on CAs to insure for the users' loss.[64]

D. E-Commerce Consumer Protection Act

Protection of consumers in business-to-consumer (B-to-C) transactions was one of the top priorities in E-commerce legislation in Korea. For this reason, the ETFA established initial provisions for consumer protection. To strengthen

---

53 *Id*. art. 26-2.

54 *Id.* art. 3.

55 *Id.* art. 4. These entities were responsible for issuing authorized certificates. *Id.* art. 14, § 1.

56 DSA, *supra* note 11, Act No. 5792, art. 3 (1999).

57 *Id.*

58 *Id.*

59 *Id.* art. 15. Article 15 provides detailed requirements for issuing the digital signature's authorized certificate. *Id.*

60 *See* 2001 UNCITRAL Model Law on Electronic Signatures, *supra* note 12.

61 DSA, *supra* note 11, at Act No. 6585 (2002).

62 *Id.* at Act No. 7428 (2006).

63 *Id.* art. 6.

64 *Id.* art. 11 (providing for corrective action for violations of the requirement in Article 25 of the DSA that all licensed CAs subscribe to an insurance program covering for damages caused in connection with their performance of certification work).

these protections, the Korean Fair Trade Commission (FTC) committed to the enactment of the Act on the Consumer Protection in Electronic Commerce (ECCPA) in 2002.[65] The ECCPA aims to protect consumers not only in E-commerce but also in transactions with distant businesses through mail order or other purchase methodologies.[66]

The ECCPA covers such topics as consumer protection in use of E-documents, the duty to preserve transaction records, prevention of errors in E-commerce, a cooling-off period for consumers, making electronic payment more reliable, the duty to insure or guaranty payment, and restricting the use of customer information.[67]

The legislature amended the ECCPA in 2005[68] and 2012.[69] The 2005 amendment introduced an escrow system for payment in E-commerce.[70] Under the escrow system, a trusted third party may hold contract money on behalf of the buyer and release it to the seller only when the ordered good is delivered to the buyer.[71] The 2005 Amendment also sought to restrict spam mail.[72] It introduced a registration system for consumers who did not wish to receive commercial emails.[73] Sellers may not send unsolicited emails to registered consumers.[74]

The 2012 Amendment to the ECCPA imposed certain additional duties on E-commerce operators and distant sellers.[75] It also required dispute mediation organizations to report the results and processes of arbitration to the FTC or to the local government to which the case was referred.[76]

E. Electronic Financial Transaction Act

For safer financial transactions in E-commerce, the Financial Services Commission (FSC) proposed the Electronic Financial Transaction Act (EFTA), which came into force in 2007.[77] The purpose of the EFTA is to establish the rights and liabilities of consumers and other participants in E-financial

---

65 ECCPA, *supra* note 8, at Act No. 6687 (2002).

66 *Id.*

67 *Id.* art. 1 ("The purpose of this Act is to protect the rights and interests of consumers by regulating the matters relating to the fair trade of goods and services by means of electronic commerce transaction, mail order, etc., and to contribute to the sound development of national economy by enhancing market confidence.").

68 *See id.* at Act No. 7487 (2005).

69 *See id.* at Act No. 11461 (2012).

70 ECCPA, *supra* note 8, at Act No. 7487, art. 24 (2005).

71 *Id.* art. 13.

72 *Id.* art. 24-2.

73 *Id.*

74 *Id.*

75 *See, e.g.*, ECCPA, *supra* note 8, at Act No. 11461, art. 5 (2012).

76 *Id.* art. 33, § 5.

77 *See* EFTA, *supra* note 9, at Act No. 7929 (2006).

transactions to ensure the safety and reliability of such transactions.[78] The EFTA applies to all E-financial transactions except certain transactions between financial institutions and E-financial business operators.[79] The key provision of the EFTA deals with strict liability of financial institutions or E-financial business operators.[80] Under this provision, financial institutions and E-financial business operators are liable for indemnifying users for losses caused by forgery, by altering the means of access to online transactions, or for damages incurred while electronically transmitting or processing a contract or transaction request.[81] They may require the user to bear the liability for such losses only if the incident was caused by the user's intention or gross negligence and the user executed a prior agreement to that effect.[82] Also, under the EFTA the FSC compelled the parties of electronic financial transactions to use an Accredited Certificate issued by an Accredited CA under the DSA.[83]

III. KOREAN LAW FOR PRIVACY & SECURITY PROTECTION IN E-COMMERCE

A. The Concept and Relevant Legislations

The right of privacy is one of the fundamental rights in the Korean Constitution.[84] The right of privacy of personal information is understood "as the ability of an individual to control the terms under which their personal information is acquired and used."[85] The concept of security protection is used in this Article to mean prevention of any "attempted access to personal information by unauthorized others."[86] In addition to the aforementioned E-commerce laws, privacy and security protection in E-commerce has been comprehensively ensured

---

[78] *Id.* at Act No. 8387, art. 1 (2006). E-financial transactions, like E-commerce transactions, involve electronic contracts and digital signatures. The EFTA provides further evidence of Korea's dedication to consumer protection both in general commerce as well as in the electronic financial industry.

[79] *Id.* art. 3.

[80] *Id.* art. 9.

[81] *Id.*

[82] *See* EFTA, *supra* note 9, at Act No. 8387, art. 9 (2006).

[83] *Id.* art. 21, § 3.

[84] *See* 1948 DAEHANMINKUKHUNBEOB [HUNBEOB] [CONSTITUTION] art. 17 (S. Kor.) ("The privacy of no citizen may be infringed.").

[85] Mary J. Culnan & Pamela K. Armstrong, *Information Privacy Concerns, Procedural Fairness, and Impersonal Trust: An Empirical Investigation*, 10(1) ORG. SCI.104, 104-05 (1999).

[86] *See* Act on Promotion of Information and Communications Network Utilization and Information Protection, Etc., Act No. 6360, Jan. 16, 2001, *amended by* Act No. 11322, art. 28-2, Feb. 17, 2012 (S. Kor.), *translated in* Korean Legislation Research Institute online database, http://elaw.klri.re.kr/eng_service/lawView.do?hseq=25446&lang=ENG [hereinafter INPIPA].

by other general legislation such as the Internet Network Protection & Private Information Protection Act (INPIPA) and the Private Information Protection Act (PIPA), which are further discussed in the following sections.

B. Legislations for Security in E-Commerce

The first Korean legislation on information networks was introduced in 1987.[87] This predecessor to INPIPA has a general clause for network security and privacy. The legislature amended the Act in 2001, changing its name to INPIPA and substantially improving security and privacy protections on the Internet. INPIPA has detailed provisions to secure network stability and the reliability of information.[88] INPIPA prohibits hacking and other intrusive acts against the network and the information distributed thereon.[89] INPIPA is enforced by criminal sanctions as well as civil penalties.[90] Through its provisions, INPIPA supplements the duty imposed by the DSA on Accredited CAs to take protective measures for E-commerce security, and it also furthers the mission of the FAEDT to improve security in E-commerce.

Not only has the legislature extended security protections in E-commerce, but recent efforts have specifically devoted resources to security in E-finance as well. The legislature amended the EFTA in 2013 to combat hacking.[91] The amended EFTA made it clear that financial institutions are legally responsible for hacking incidents, which ensures secure transactions.[92] The amendment also requires the FSC and financial companies to immediately respond to attacks on the E-financial infrastructure.[93] An amendment to the EFTA in 2015 introduced more stringent regulation on lending or renting means of access and bank accounts in order to prevent misuse of bank accounts.[94]

C. Legislations for Privacy Protection in E-Commerce

Over the past 20 years, legislation has expanded the scope of privacy protections for consumers in Korea. The E-Documents Act was the first legislation that protected privacy in E-commerce.[95] The DSA also imposes a duty to protect privacy of users.[96] INPIPA introduced more than ten new sections for

87 *Id.* at Act No. 3848 (1986).
88 *Id.* at Act No. 6360 art.45 (2001).
89 *Id.* art. 48.
90 *Id.* arts. 64-3, 70-76.
91 *See* EFTA, *supra* note 9, at Act No. 11461 (2013).
92 *Id.* at Act No. 8387, art.21 (2012).
93 *Id.*
94 *Id.* at Act No. 12837, art.40 (2014).
95 E-Documents Act, *supra* note 7, at Act No. 11461, art.1 (2012).
96 DSA, *supra* note 11, at Act No. 5792 (1999).

protecting the privacy and secrecy of users of internet services.[97] INPIPA also required that information service providers who intend to make cross-border transfers of personal information of a user must obtain consent of the user and must take protective measures.[98] The ECCPA, the statute for E-commerce consumers, specifically prohibits E-commerce operators and distant sellers from using consumer information without consent or beyond the scope of the consent given.[99]

D. Private Information Protection Act (PIPA)

As comprehensive personal privacy protection legislation, PIPA was finally enacted in 2011 after long discussions.[100] PIPA confers citizens' full rights to control private information—a response to the Korean Constitutional Court's decision declaring that a person's right to control her own private information is a fundamental constitutional right.[101] PIPA replaced the existing Public Agency Information Protection Act and part of the INPIPA. It also prevails over other laws such as the Credit Information Protection Act.[102]

PIPA targets all information processors, regardless of whether they are public or private, electronic or manual.[103] PIPA defines the personal information that it protects as information that pertains to a living person, including her full name, resident identification number, images, and so on, and any combination of these markers by which the individual can be identified (including information by which the individual in question but can be identified only through simple combinations with other information).[104] Protection under PIPA extends to so-called "sensitive information," which is "any information on thought, beliefs, joining or withdrawal from a labor union or political party, a political opinion, health, sexual life, etc., which could substantially infringe on the privacy of the subject of the information."[105] Information processors are not allowed to process such information unless the law so requires or the information holder consents.[106]

PIPA established the Personal Information Dispute Mediation Commission, which is empowered to treat both public and private sector

---

97 INPIPA, *supra* note 86, at Act No. 11322 (2012).

98 *Id.*

99 ECCPA, *supra* note 8, at Act No. 6687 (2002).

100 Personal Information Protection Act, Act No. 10465, Mar. 29, 2011, *amended by* Act No. 11990, Aug. 6, 2013 (S. Kor.), *translated in* Korean Legislation Research Institute online database, http://elaw.klri.re.kr/eng_service/lawView.do?hseq=28981&lang=ENG [hereinafter PIPA].

101 Constitutional Court Decision, May 26, 2005. 99 HUNMA 513, 2004 HUNMA 190 followed by Supreme Court case, 2008Da42430, (Sept. 2, 2011).

102 PIPA, *supra* note 100, at Act No. 11990, art.6 (2013).

103 *See id.* at Act No. 11990 (2013).

104 *Id.* art. 2, § 1.

105 *Id.* art. 23.

106 *Id.*

disputes.[107] Also, collective mediation procedures are available for information holders who are subject to large-scale impacts but minimal damage.[108] Consumer organizations may file a collective action for the suspension or injunction of activities, which violate privacy and information protection law following a mandatory collective mediation procedure.[109]

The legislature amended PIPA in 2013 and 2014 because of repeated mass leaks of resident ID numbers that information processors held.[110] These amendments prohibit information processors from collecting and processing resident ID numbers while also requiring them to encrypt resident ID numbers that they have already collected.[111]

E. Evaluation of Korean Legislation

When analyzing the Korean legislative efforts to improve security and privacy in the context of electronic transactions, two primary observations become critical for identifying areas for improvement. As complex as the above legal framework is, it is made more so by the fact that different ministries are responsible for enforcing each law. As explained above, Korea has many different and complicated laws for privacy and security in E-Commerce. The relevant parties to E-Commerce have been confused and irritated due to complex regulations from various different governmental agencies. The Ministry of Industry and Trade enforces the FAEDT.[112] The Ministry of Future, Creation and Science enforces the DSA and INPIPA.[113] The Fair Trade Commission is in charge of enforcement of the ECCPA.[114] The Financial Service Commission regulates electronic financial transactions under the EFTA.[115] Finally, the Ministry of Government Administration & Home Affairs recently joined this power game by taking charge of PIPA.[116] Each of these ministries enforces its statute independently without coordination or cooperation with the other ministries. This adds an additional layer of confusion for E-commerce participants, who are already confused and irritated by the intricate regulations of

---

[107] PIPA, *supra* note 100, at Act No. 11990, arts. 40, 43 (2013).

[108] *Id.* art. 49.

[109] *Id.*

[110] Hee-Eun Kim, *Korea Strengthens Protection for "Resident Registration Numbers" (RRNs): Leaks May Face a Fine of up to 0.5 Billion Korean Won*, INSIDE PRIVACY (Aug. 7, 2013), http://www.insideprivacy.com/international/korea-strengthens-protection-for-resident-registration-numbers-rrns-leaks-may-face-a-fine-of-up-to-0/.

[111] PIPA, *supra* note 100, at Act No. 11990, art. 24 (2013).

[112] *See* E-Documents Act, *supra* note 7, at Act No. 11461, art. 1 (2012).

[113] *See* DSA, *supra* note 11, at Act No. 5792 (1999); INPIPA, *supra* note 86, at Act No. 11322 (2012).

[114] *See* ECCPA, *supra* note 8, at Act No. 6687 (2002).

[115] *See* EFTA, *supra* note 9, at Act No. 11461 (2013).

[116] *See* PIPA, *supra* note 100, at Act No. 11990 (2013).

the many laws discussed above. Therefore, there is a need to regulate E-commerce privacy and security under a unified policy and legislation.

The other observation on the relevant Korean laws is that E-commerce is strictly regulated for privacy and security protection. As mentioned above, in order to make any electronic payment or electronic financial transaction, users are required to use a certificate issued by an Accredited CA.[117] A foreign consumer could not purchase an item from a Korean E-commerce operator because he was not allowed to use the service of a Korean Accredited CA. Due to criticism from the business community, the EFTA was amended in 2014 to repeal the stringent requirement and allow financial companies to install alternative financial security means as appropriate.[118] However, the requirement to use an Accredited Certificate issued by an Accredited CA in other E-Commerce still remains.[119] As a result, the government regulation of E-commerce for privacy and security protection is still too stringent and continues to hinder E-commerce developments.

IV. UNITED STATES AND EUROPEAN UNION LAW FOR PRIVACY AND SECURITY PROTECTION IN E-COMMERCE

A. International Developments

International E-commerce has developed not by norms but by practice. The Society for Worldwide Interbank Financial Telecommunications (SWIFT) has made most international funds transfers.[120] SWIFT has thus provided a network enabling world financial institutions to send and receive information in a standardized, secure, and reliable environment.[121] However, neither UNCITRAL nor any other organization has established international norms on E-commerce privacy and security. What follows briefly reviews the highly regarded E-commerce legislation on privacy and security in the United States and the EU.

B. U.S. Law for Privacy & Security Protection in E-Commerce

In the United States privacy is largely a matter of economics rather than a matter of law. Once an individual provides information, except certain information such as medical records, to an E-commerce operator, all rights to that information are lost. Only operators' self-regulation for privacy protection is enforceable. Therefore, they are responsible only when they violate their own privacy statements or policies. However, the United States does regulate

---

117 *See supra* Part II.C.

118 EFTA, *supra* note 9, at Act No. 7929 art. 21 §§ 2-3 (2006).

119 *Id.*

120 *Society for Worldwide Interbank Financial Telecommunications—SWIFT*, INVESTOPEDIA, http://www.investopedia.com/terms/s/swift.asp (last visited Nov. 12, 2015).

121 *Id.*

unauthorized collection of personal information on the Internet. The U.S. Congress enacted the Electronic Communication Privacy Act of 1986 (ECPA) to protect privacy in electronic communication.[122] The ECPA basically prohibits access to stored E-communications and restricts the government from using wiretaps on transmission of electronic data.[123] The ECPA allows the government to demand that service providers hand over personal consumer data.[124] It also has pen register and trap and trace provisions, which permit tracing of telephone communications under some circumstances.[125] A piece of controversial legislation that further threatens the right of privacy is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act). The Act allowed roving wiretaps, searches of business records, and surveillance of the individuals suspected of terrorist-related activities not linked to terrorist groups, so-called "lone wolves."[126] The USA Freedom Act of 2015 amended the USA PATRIOT Act to prohibit the National Security Agency (NSA) from continuing its unrestricted mass email data collection.[127] It also prohibits communication companies from retaining the data from which the NSA obtains information unless a federal court so permits.[128]

C. European Union Law for Privacy & Security Protection in E-Commerce

In the EU, privacy protections have been more expansive. The first privacy protection legislation was the Data Protection Directive 95/46/EC ("DPD").[129] The European Parliament established the DPD to provide a regulatory framework to: (1) guarantee secure and free movement of personal data across the national borders of the EU member countries; and (2) set a baseline of security around personal information wherever it is stored, transmitted, or processed.[130] The DPD prohibits processing personal data except when the processor meets certain conditions. These conditions fall into three categories: transparency, legitimate purpose, and proportionality.[131] Member States must also

[122] ECPA, *supra* note 14.

[123] *Id.*

[124] *Id.*

[125] *Id.*; 18 U.S.C. § 3121.

[126] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001) [hereinafter USA Patriot Act].

[127] Uniting and Strengthening America by Fulfilling Rights and Ensuring Effective Discipline Over Monitoring Act of 2015, Pub. L. 114-23, 129 Stat. 268 (2015) [hereinafter USA Freedom Act].

[128] *Id.*

[129] Council Directive 95/46/EC of Oct. 24, 1995, Data Protection Directive, 1995 O.J. (L 281) (EC) [hereinafter DPD].

[130] *Id.*

[131] *Id.*

prohibit processing of sensitive personal data.[132] The EU set up the safe harbor arrangement with the United States in 2000 under which U.S. companies are allowed to self-certify compliance with the standards of the EU DPD and have freely transferred personal data from the EU to the United States.[133]

In order to cope with the needs for data protection and privacy in the digital age, the European Parliament supplemented the DPD with the passage of the E-Privacy Directive 2002 (EPD).[134] The EPD regulates a number of important issues, such as confidentiality of information, treatment of traffic data, spam, and cookies.[135] Contrary to the DPD, which specifically addresses only individuals, the EPD applies to legal persons as well.[136]

The EPD imposes general obligations on information service providers to provide security of services. It also obligates these providers to maintain the confidentiality of information.[137] Member States are required to prohibit listening, tapping, storage, or other kinds of interception or surveillance of communication and "related traffic," unless the user consents or meets prescribed conditions.[138] The EPD requires providers to erase or anonymize traffic data and to introduce an opt-in regime for unsolicited emails.[139] Directive 2009/136 ("Cookie Directive") amended the EPD.[140] It made several changes, especially concerning cookies, which are subject to the user's prior consent.[141]

D. Conflicts Between U.S. Privacy Law and European Union Privacy Law

We can observe from the above introduction of the United States and EU law that regulations of E-commerce in the United States is much looser than in the European Union. Generally, data privacy law in the United States is to some extent behind the stricter and clearer requirements of the DPD and other directives. It is hard to find a legal system that regulates E-commerce operators more strictly than the EU's. Korea follows the European approach but is less protective of privacy. In 2013, it was revealed the NSA has run numerous global surveillance programs to which many U.S. telecommunication companies

---

132 *Id.*

133 Commission Decision 2000/520/EC of July 26, 2000, O.J. (L 215) (EC) (detailing the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the U.S. Department of Commerce).

134 Council Directive 2002/58/EC of July 31, 2002, E-Privacy Directive, 2002 O.J. (L 201) (EC) [hereinafter EPD].

135 *Id.*

136 *Id.*

137 *Id.*

138 *Id.*

139 EPD, *supra* note 134.

140 Council Directive 2009/136/EC of Nov. 25, 2009, O.J. (L 337) (EC) [hereinafter Cookie Directive].

141 *Id.*

voluntarily cooperated.[142] As noted earlier, the same surveillance was made by the Korean intelligence agency. On October 9, 2015, the European Court of Justice (ECJ) invalidated the U.S.-EU safe harbor arrangement. The ECJ viewed that the United States has allowed large-scale collection and transfer of personal data without proper means of redress or effective judicial protection for EU citizens, that the safe harbor arrangement lacked the requisite guarantees of privacy protection, and that its later implementation by the United States did not meet the requirements of the DPD.[143] Progressive steps for privacy protection must resolve this conflict. The ECJ judgment demonstrated the essential need to respect the privacy right of the information holders in communication and the need for more responsibility of E-Commerce operators for privacy and security. In this respect, Korean E-Commerce law on privacy protection should be improved as discussed below.

V. PROPOSALS FOR IMPROVEMENTS OF KOREAN LAW

A. New Policies for Privacy & Security Protection in E-Commerce

The world is moving quickly from E-commerce to mobile commerce.[144] Sending and receiving money on smart phones is becoming easier. Mobile payments will become more common and the check will be in the tweet.[145] Privacy and security are more vulnerable in M-commerce than in E-commerce.[146] Until now, Korean government has put stress on strengthening direct legal regulation for enhancing privacy and security.

Korea needs a new approach to privacy and security. First, the new approach must combine technology, social infrastructure and norms, the market, and the law. Privacy and security are increasingly "a complex social phenomenon

---

[142] Glenn Greenwald & Ewen MacAskill, *Boundless Informant: The NSA's Secret Tool to Track Global Surveillance Data*, THE GUARDIAN (June 13, 2013, 9:00 AM), http://www.theguardian.com/world/2013/jun/08/nsa-boundless-informant-global-data mining.

[143] *European Court of Justice Invalidates U.S.–EU Safe Harbor* Agreement, NAT'L L. REV. (Oct. 9, 2015), http://www.natlawreview.com/article/european-court-justice-invalidates-us-eu-safe-harbor-agreement.

[144] M-commerce, like E-commerce and f-commerce, also involves electronic transactions, specifically those involving mobile phones. Although many of the laws in Korea, the United States, and the EU focus on E-commerce, the development and growing popularity of m-commerce is quickly demonstrating the increasing need for further regulations of electronic transactions in order to protect privacy and security.

[145] *The Cheque Is in the Tweet: Sending and Receiving Money on Your Smartphone is Getting Easier*, THE ECONOMIST (Nov. 22, 2014) http://www.economist.com/news/finance-and-economics/21633884-sending-and-receiving-money-your-smartphone-getting-easier-cheque.

[146] Users of mobile phones tend to not tolerate any compulsory use of the certified digital signature.

with interactions among new technologies, regulatory structures, and citizens' perceptions of privacy and social norms."[147] New policies for privacy and security protection in M-commerce and E-commerce should be designed in consideration of all these factors. Second, the new approach must also balance the promotion of E-commerce with privacy and security concerns. Governments should establish appropriate policy and enforcement schemes for such balance utilizing various options to accomplish the goal without sacrificing the privacy of E-Commerce consumers.

B. Measures to Improve Privacy Protection in E-Commerce

Legal measures by themselves are not enough to fully protect privacy in E-commerce. The government must encourage the development of technologies that can protect privacy and enhance the information holders' capability to control its personal information. For example, a new Korean mobile app called KIPI enables peer-to-peer (P2P) communications without providing cell phone numbers or other personal information.[148] By using the KIPI App, the service users themselves can create, store, transmit, and even delete communications at will.[149] The government should invest in, or provide incentives for research and development of similar advanced technologies to improve privacy.

Consumers also should pay more attention to their own privacy and should adopt updated technical mechanisms that protect their privacy. They should learn the options they have for more secured E-commerce transactions.

C. Measures to Improve Security Protection in E-Commerce

It is largely accepted in Korea that the country has relatively few experts in cyber security. The government is considering measures to encourage education of cyber security experts. Such new policies by the Korean government are desirable. The private sector should adopt more security measures and hire more cyber security experts. In other words, E-commerce operators should pay more attention to their own security.

Some argue that requiring the use of an Accredited Certificate for digital signatures does not help to improve security in E-commerce.[150] Rather, the argument goes, such cumbersome requirements hinder expansion of trade volume

---

[147] Mark S. Ackerman & Donald T. Davis, Jr., *Privacy and Security Issue in E-Commerce*, THE NEW ECONOMY HANDBOOK 9, http://econ.ucsb.edu/~doug/245a/Papers/ECommerce%20Privacy.pdf (last visited Nov. 12, 2015).

[148] Ham Jong-Sun, *Tapping Your Smartphone Is Easy, But Protecting Yourself Is Easy Too*, KOREA JOONGANG DAILY (Aug. 7, 2015), http://koreajoongangdaily.joins.com/news/article/Article.aspx?aid=3007618.

[149] *Id.*

[150] *See supra* Part III.E.

in E-commerce.[151] Following this logic, E-commerce operators may consider easing the use of secured digital signatures, instead simply insuring against the risk of a damages caused by a lax security system.

The government should admit its limitation to guarantee secured E-commerce. The government must adopt policies and enforcement mechanisms that grant more authority to the private sector in determining the security level. But at the same time, the government must establish legal remedies for consumers to take legal action against E-commerce operators who fail to protect their consumers.

D. Contribution for Global Uniform E-Commerce Rules

Global uniform E-commerce laws facilitate international E-commerce. But, as mentioned above, there are few international norms applicable to privacy and security for cross-border E-commerce. For this reason, the EU has sought a uniform standard for privacy and security in E-commerce by requiring countries outside of its membership to have data protection as "adequate" as that of the DPD.[152] The European Commission for the Protection of Privacy has prepared a "white list" of countries in which EU citizens' personal data can be exported without any further safeguard measure.[153] These efforts, however, fall far short of establishing global uniform rules for privacy and security.

Korea ought to contribute to global uniform E-commerce rules by formulating appropriate internal rules for E-commerce privacy and security. These rules need to consider the possibility that uniform rules for privacy and security of E-commerce may develop. However, only some areas of the law are conducive to uniform global policy. For example, a uniform rule that prohibits government or E-commerce operator violations of privacy is realistic. However, establishing a uniform rule for security in E-commerce, such as prohibition of hacking, will be more difficult. For this purpose, coordination of governmental policies for Internet business and for national security must be considered when making internal politics. Thus, Korea should make its contribution to uniform E-commerce regulations through internal legislation drafted in light of the global privacy and security environment.

In addition, Korean E-commerce law should be consistent with upcoming uniform rules for global E-commerce. Uniform global E-commerce rules should not become entangled with sensitive political issues, such as governmental security and traders' privacy concerns. As a first step, a uniform choice of law rule for cross-border E-commerce should be formulated by international communities such as The Hague Conference for Private International Law in

---

[151] *Id.*

[152] DPD, *supra* note 129; *see also Transfers Outside the EU with Adequate Protection*, COMMISSION FOR THE PROTECTION OF PRIVACY (2015), http://www.privacycommission.be/en/transfers-outside-the-eu-with-adequate-protection.

[153] *Transfers Outside the EU with Adequate Protection*, *supra* note 152.

cooperation with the UNCITRAL. A comparative study of trans-pacific E-commerce rules and practices, especially on unfair commercial conduct, could lead to the formulation of the best E-commerce practices enforceable by private institutions such as national chambers of commerce.

Also, cross-border E-commerce rules may be considered to be included as integral parts of Free Trade Agreements. The policy makers for the Free Trade Agreement in each country should be aware that the volume of E-commerce will soon surpass the volume of traditional trade.

VI. CONCLUSION

I propose improvements to Korean E-commerce laws that attain a proper balance between the promotion of E-commerce and privacy and security protections. It requires social interactions among the development of new technologies, regulatory structures, and citizens' perceptions of privacy and social norms. The Korean government must not only improve its legal structure, it must also pay attention to social norms such as its citizens' perceptions of privacy and the development of technology that improves privacy and security in E-commerce. Meanwhile, it would be a positive step for Korea and other nations to start the process of identifying uniform choice of law rules for cross-border E-commerce, based upon best practices and enforceable by chambers of commerce and other private and public law institutions.