8-1-2003

Protection of Consumer Privacy in E-commerce

Choong L. Ha
University of Georgia School of Law

PROTECTION OF CONSUMER PRIVACY IN E-COMMERCE: THE U.S. AND KOREA

by

CHOONG LYONG HA

(Under the Direction of Professor Gabriel M. Wilner)

ABSTRACT

Among the negative effects on Internet consumers, the divulgence of personal information to the public has been reported as one of the most serious infringements on consumer rights. Both consumers and sellers around the world have sought to come up with an optimal solution for information privacy. Several incompatible characteristics of regulating consumer privacy in e-commerce between the U.S. and Korea were explored, and curative suggestions were made to establish a new legal framework to protect online consumer privacy. First, Korea's regulations for protecting online consumer privacy were found to be centrally controlled, while the U.S. authorities have encouraged self-regulation. Considering the long run efficiency of self-regulation, the Korean authorities should seek more self-regulatory measures and establish consensus among the businesses to voluntarily protect consumer online privacy. Second, U.S. regulations on protection of online consumer privacy are for the most part commercially oriented and controlled by the FTC, whereas in Korea, an administrative department, the Ministry of Information and Communication, regulates online consumer privacy as a primary authority, resulting in lack of specialization in the matters of consumer protection. To improve the efficiency and specialization in regulation of online consumer privacy in Korea, it would be necessary to promulgate a directive specially designed for protecting consumer privacy and delegating the regulatory power to the Korea Consumer Protection Agency established by the Consumer Protection Act. Finally, international arbitration is recommended as the best tool to resolve and prevent the intricacies of international litigation brought against violation of online consumer privacy.

INDEX WORDS: Consumer privacy, Protection of consumer information, E-commerce, International jurisdiction, Cyberspace, Online Privacy, Consumer Protection, International arbitration.

PROTECTION OF CONSUMER PRIVACY IN E-COMMERCE: THE U.S. AND KOREA

by

CHOONG LYONG HA

Ph.D., The University of Texas at Arlington, 1998

Bachelor of Laws, Korea National Open University, Korea, 2002

A Thesis Submitted to the Graduate Faculty of The University of Georgia in Partial Fulfilment of the Requirements for the Degree

MASTER OF LAWS

ATHENS, GEORGIA

2003

PROTECTION OF CONSUMER PRIVACY IN E-COMMERCE: THE U.S. AND KOREA

by

CHOONG LYONG HA

Major Professor: Gabriel M. Wilner

Committee: Robert D. Brussack

Electronic Version Approved:

Maureen Grasso
Dean of the Graduate School
The University of Georgia
August 2003

DEDICATION

To the glory of Jesus Christ

ACKNOWLEDGMENTS

This thesis could not have been completed without my wife's perseverance during the LL.M. year. My father and mother would be the ones congratulating me with their whole hearts on this academic achievement. Professor Gabriel Wilner has guided me academically and supported me financially. Professor Robert Brussack allowed me to input his cutting-edge information into the thesis. Professor Eun Sup Lee has encouraged me to keep a right track of my academic career.

With love to Solomon and Rebecca.

TABLE OF CONTENTS

CHAPTER 1

INTRODUCTION

With the advent of the Internet, the means of communication in commercial transactions has been significantly changed, shifting from paper-based documents to the newly emerging online-based data files. Considering the expected growth in Internet transactions,[1] this trend is likely to be intensified for decades to come.

Now, with the help of the diffusion of the Internet throughout the world, individual consumers have far more access to international electronic transactions. In order to purchase goods through the Internet, the only thing they need to do is to transmit their personal information (including name, address, and credit card number, etc.) to the online seller. International electronic commerce provides a variety of opportunities to businesses and while giving consumers more product choices, faster transactions, greater convenience and lower costs.[2]

However, the expansion of electronic commerce (hereinafter "e-commerce") has not always been favorable to the consumers, because consumers have been exposed to more risks associated with electronic transactions. For instance, when the consumers search the Internet

---

[1] *See*, Mozelle W. Thompson, *Presentation: The Challenges of Law in Cyberspace- Fostering the Growth an Safety of E-Commerce*, 6 B. U. SCI. & TECH. L. 1, 2 (2000).

[2] *See*, Tapio Puurunen, *The Legislative Jurisdiction of States over Transactions in International Electronic Commerce*, 18 J. MARSHALL J. COMPUTER & INFO. L. 689, 689 (2000).

for online shopping, they have to make their purchase decisions based only on the online information provided by the sellers, which sometimes may be distorted or even fraudulent. In addition, when consumers transmit their personal information to the Internet sellers to complete the buying contract, they may be put in danger that their personal information will be disclosed by the data collectors to third parties.

Among these negative effects on Internet consumers, the divulgence of personal information to the public has been reported as one of the most serious infringements on consumer rights.[3] Most consumers are definitely concerned about the protection of personal information submitted during the course of e-commerce.[4] Furthermore, 82 % of the American adults surveyed responded that protection of privacy is a key factor in deciding whether they become member of a website that requires them to submit personal information.[5]

The U.S. is not the only country concerned about online privacy, because protection of consumer information has become a global issue. Both consumers and sellers around the world have sought to come up with an optimal solution for information privacy. For example, the European Union issued the data protection directive to deal with privacy problems in the Internet.[6] The EU Directive strictly regulates infringements on the privacy rights of EU citizens with a view towards protecting personal information. Recently, Korean consumers have been shocked by the unauthorized withdrawal from an automated teller

---

[3] *See*, Mozelle W. Thompson, *supra* note 1, at 4 ("Data protection was among the first policy issues to surface as e-commerce started to become a reality").

[4] *See*, *e.g.*, Joe Queenan, *My Mail Insecurity; What If the Neighbors See What the Junk Marketers Send Me?*, The Wash. Post, Oct. 22, 1995, at C5.

[5] *Business Week/Harris Poll: Online Insecurity*, Business Week, March 16, 1998, at 102.

[6] *See*, Council Directive 95/96, 1995 O.J. (L 281) 31.

machine by someone using a stolen password and a forged ATM card,[7] which raises an obvious cause of concern about the security of personal information provided to businesses including banks and government agencies.[8]

The main purposes of this research are threefold. First, regulations concerning online consumer privacy will be compared between the U.S. and Korea to address compatibilities and incompatibilities, with curative measures sought for conflicts between the two sets of regulations. Second, the legal issues of international jurisdiction with respect to online consumer privacy in e-commerce between the U.S. and Korea will be explored to see how jurisdictional principles differ between the two countries. Third, the thesis will discuss what kind of dispute resolution method would be most appropriate for disputes arising between the U.S. and Korea regarding online consumer privacy.

To accomplish these research goals, this study will be conducted through investigation and analysis of the primary sources of regulation in each country, including codified rules, governmental directives, and judicial cases as the primary sources of regulation. In addition, several viewpoints on online consumer privacy provided by lawyers will be reviewed and discussed to make the research more balanced in its arguments.

---

[7] Jung Hee Lee, *A Desperate Measure to Cope with Illegal Dissemination of Bank Passwords*, The Pusanilbo, Jan. 22, 2003, at 35.

[8] It seems ironical that this electronically schemed larceny was committed only two days after the revised Act on the Promotion of Use of Information Network and the Protection of Information came into effect and the government launched a massive crackdown on infringe of privacy by spam mails.

CHAPTER 2

LEGAL FOUNDATIONS OF CONSUMER PRIVACY IN E-COMMERCE

A. E-Commerce

1. Backgrounds

With the help of the popularization of the Internet, e-commerce enthusiasm has been spread over almost all economic activities. Due to the multidimensional utility of the Internet business, it is not easy to provide an uniform definition of e-commerce. For instance, the systems regarding Internet business can be classified into three categories including business-to-business, business-to-consumer, and 'intra-enterprise'.[9]

Irrespective of the multi-dimensionality of e-commerce, some experts have tried to sort out its common elements.[10] While it may be impossible to define e-commerce with perfect uniformity, two common features seem worthy of notice. One is that e-commerce is based on an electronic communication network acting as intermediary. Therefore, in order for a

---

[9] WASHIM E. RAJPUT, E-COMMERCE SYSTEMS ARCHITECTURE AND APPLICATIONS 2 (2000) (He provides the definitions of each systems as following: "Business to business e-commerce is a system that enables an organization to transact with other organizations for its business activities (e.g., corporate procurement). Business to consumer e-commerce is a system that enables an organization to sell goods and services through the Internet to public customers. Intraenterprise e-commerce is a system to connect an organization's internal activities (e.g. enhanced information sharing)").

[10] *See*, MICHAEL R. SOLOMON & ELNORA W. STUART, MARKETING 190 (2nd ed. 2000) (stating that "Electronic commerce or e-commerce is the buying and selling of products electronically, usually via the Internet."); *see* also CRAIG STANDING, INTERNET COMMERCE DEVELOPMENT 4 (2000) ("Electronic commerce is the online exchange of goods, services, and money within firms and between firms and their customers.").

transaction to be called e-commerce, at least some portion of the transaction should be conducted using an electronic communication network.[11]

The other is that e-commerce should be followed by online or offline delivery of goods or services between the seller and buyer. Based on these two elements, e-commerce can be defined as the transaction of goods and services via an electronic communication network.

Electronic commerce has been adding "tremendous business values" to sellers and buyers[12] while at the same time bringing about a variety of threats. Two kinds of benefits are expected to accrue from e-commerce. First, electronic commerce leads consumers to be much more informed about the availability and characteristics of goods and services. Second, e-commerce significantly reduces transaction costs that may be incurred linking sellers with buyers by utilizing freely occupied cyberspace.[13]

However in reality, e-commerce has not always been ornamented with these rosy advantages. Several pitfalls lurking behind e-commerce may be seriously alarming to online consumers.[14] First, e-commerce requires potential customers to be equipped with costly network communication devices (e.g., computer, modem etc.). Most consumers feel that the cutting-edge communication equipment is not still readily affordable and accessible.[15]

Second, psychological impediments may block the progress of e-commerce. Many consumers are increasingly hesitant to send their credit card information to the Internet

---

[11] The term, electronic communication network, was employed to represent mostly the Internet, while it does not exclude other intermediaries (e.g., telephone, electronic data interchange, etc.).

[12] GARTH SALONER & A. MICHAEL SPENCE, CREATING AND CAPTURING VALUE 43 (2002).

[13] *Id*.

[14] *See*, GARY P. SHNEIDER & JAMES T. PERRY, ELECTRONIC COMMERCE 13 (2001).

[15] *Id*.

vendor. They are also still resistant to changes in shopping behavior and feel uncomfortable selecting merchandise without personal contact.[16]

In addition, the legal environment of e-commerce has been changing too fast for anyone to keep up with it; thus, e-commerce regulations have been easily outdated and endangered with unrealistic conditions.[17] Because the technology of e-commerce improves rapidly, it seems necessary for the related regulations to be updated and revised periodically in order to reflect the trend in the technological change. Furthermore, if e-commerce is conducted internationally, the legal environment is likely to be more complicated due to the addition to the transaction of choice of law and jurisdictional issues.

2. Legal Issues

Traditional regulations on businesses have been faced with a large-scale modification in order to cope with the introduction of the Internet into commercial transactions.[18] For instance, the regulatory scope of intellectual property rights has been expanded into new legal areas including online copy-right, domain names, etc. While it may be destined that the existing regulations be revised, the fundamental or constitutional principles to protect individual legal rights have remained unchanged. Accordingly, it would be reasonable that

[16] *Id*. at 14.

[17] *Id.*

[18] Pamela Samuelson, *Five Challenges for Regulating the Global Information Society*, *in* REGULATING THE GLOBAL INFORMATION SOCIETY 311, 317 (Christopher T. Marsden ed., 2000).

new regulations should not "overreact"[19] in dealing with the recent problems occurring due to the advent of e-commerce.

It is also a notable legal issue that e-commerce should be dealt with in the context of international laws, whether or not the transaction is domestic or international, because the Internet can reach any part of a world without boundaries.[20] Considering the lack of boundaries in the Internet, it will be a challenge to the international lawyers that the principles of international jurisdiction with respect to Internet transactions has yet to be clarified in terms of territory, because jurisdiction has traditionally been tied with physical geography.

Consumer protection in cyberspace has been an active regulatory target. For example, the FTC broadened its regulatory power into Internet business activities.[21] In addition to such empowerment of the FTC in regulation of e-commerce, several statutes have been enacted to regulate business' activities in the Internet, including the Children's Online Privacy Protection Act[22] and the Anticybersquatting Consumer Protection Act.[23] Other regulations concerning consumer protection are related to Internet advertisement[24] and "spamming"[25]

Among the regulations in e-commerce that are not intended to protect individual consumers, the protections of domain names and copy right in cyberspace may nonetheless be recognized as critical to businesses employing Internet tools.[26] Currently registration and

---

[19] *Id.*, at 319.
[20] *Id.*, at 323.
[21] 15 U.S.C. §§ 41-58 (2001).
[22] 15 U.S.C. §§ 6501-6506 (2001).
[23] 15 U.S.C. § 1125(d) (2001).
[24] GERALD SPINDLER & FRITJOF BÖRNER, E-COMMERCE LAW IN EUROPE AND THE USA, 708 (2002).
[25] *Id.*, at 712.
[26] *Id.*, at 720-732.

control of domain names is conducted by the National Science Foundation (NSF), Network Solutions Inc.(NSI) and Internet Corporation for Assigned Names and Numbers (ICANN).[27] To protect online copyright, the Digital Millennium Copyright Act (DMCA) was effectuated on October 28, 1998.[28]

B. Consumer Privacy

1. Concepts of Consumer Privacy

To define consumer privacy, the concept of privacy should first be clarified. This idea of privacy may be historically traced back[29] to 1890 as the legal notion of the "right to be let alone"[30]. Although it had not been referred to as privacy, the suggested notion seems sufficiently inclusive of the key legal aspects of privacy in current use in that it was understood as an individual right vested in personal information.

In *United States Dep't of Justice v. Reporters Committee for Freedom*, the U.S. Supreme Court provided a common-law based concept of privacy, which is the legal right to "encompass the individual's control of information concerning his or her person."[31] In deriving this definition of privacy, the Supreme Court did not specifically indicate that privacy is a legal right to be protected from violations. However, based on its definition, the

[27] *Id*., at 721.
[28] 17 U.S.C. §§ 1201-1205 (2001).
[29] PAUL SHAW, E-BUSINESS PRIVACY AND TRUST 21-2, (2001).
[30] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193**,** 193 (1890).
[31] 489 U.S. 749, 763 (1989).

notion of privacy should be viewed as a legal right.[32] Thus, in broad terms, it can be said that 'privacy' and 'privacy right' have the same meaning when they are used in the context of protecting individuals from infringements on their personal information.

In addition to the legal right implied in privacy, private or personal information (another key attribute of privacy) has been recognized as an object to be protected by privacy rights under the U.S. Supreme Court's definition[33] and other sources[34] of writings on privacy. The Arizona Supreme Court held that if a piece of information is found to be private or personal, it will be endowed with "a privacy claim"[35]. The U.S. Supreme Court provided a condition for information to be private or personal, stating that " it should be intended for or restricted to the use of a particular person or group or class of person: not freely available to the public."[36]

The concept of consumer privacy should not deviate far from the traditional understandings of privacy. The only distinction between generic privacy and consumer privacy that can be made is with respect to the use of personal information. If personal

---

[32] *See*, Omar Saleem, *The Establishment of A U.S. Federal Data Protection Agency to Define and Regulate Internet Privacy and Its Impact on U.S. -China Relations: Marco Polo Where Are You?*, 19 MARSHALL J. COMPUTER & INFO. L. 172, 172 (2000); *see* also A. BRECKENRIDGE, THE RIGHT TO PRIVACY 1 (1970) ("Privacy, in my view, is the rightful claim of the individual to determine the extent to which he wishes to share of himself with others. . . . It is also the individual's right to control dissemination of information about himself"); A. WESTIN, PRIVACY AND FREEDOM 7 (1967) ("Privacy is the claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others").

[33] *See*, Pamela Samuelson, *supra* note 20 at 763.

[34] *See*, 15 U.S.C. §§ 41-58 (2001); *see also* James P. Nehf, *Recognizing The Societal Value in Information Privacy*, 78 WASH. L. REV. 1, 7 (2003) (stating that "information privacy should be viewed as a societal value justifying a resolution in the public interest, much like environmental policy and other societal concerns, with less emphasis on individual self policing and market-based mechanisms.").

[35] Scottsdale Unified Sch. Dist. No. 48 v. KPNX Broad. Co., 191 Ariz. 297, 301 (1998).

[36] 489 U.S. at 763-64 (1989). *See*, 56 F. Supp. 105, 107 (E.D.N.Y. 1991) (For instance, social security numbers and birth dates were decided as being private, thus given the privacy right to protect them from being made public.).

information is utilized in the context of commercial transactions, such information may be viewed as consumer information, which will be further vulnerable to legal concerns on ways to protect it from being made public without authorization. Slightly different from the generically defined privacy,[37] consumer privacy can be seens as a legal right to cover the consumer's control of his or her personal information.

The Federal Trade Commission Act recognizes consumer privacy as an individual right to be protected against industries.[38] According to this Act, the FTC is authorized to prevent businesses from collecting and disseminating customer personal information in unjust ways.[39] The FTC filed its "first"[40] lawsuit on consumer privacy in e-commerce against GeoCities, complaining that GeoCities was collecting and disseminating customer information in deceptive ways.[41] The case was finally settled when the defendant complied with the claimant's demand that GeoCities should expressly notify the customers of the use of their personal information on the Internet.[42]

2. Characteristics of Consumer Information

One of the most compelling forces of e-commerce is the one-on-one marketing relationship between buyers and sellers.[43] The one-on-one marketing program can not be executed without gathering consumer information as accurately as possible. In addition, by

---

[37] *See*, 489 U.S. at 763 (1989).
[38] 15 U.S.C. § 45 (a) (1994).
[39] *Id.*
[40] Debra A. Valentine, *Symposium on Internet Privacy: Privacy on the Internet: The Evolving Legal Landscape*, 16 COMPUTER & HIGH TECH. L. J. 401, 405 (May 2000).
[41] *See*, *In re* GeoCities, Inc., No. C-3849, 1999 FTC LEXIS 17 (FTC Feb. 5, 1999).
[42] *Id.*, at 19-21.
[43] Wasim E. Rajput, *supra* note 9, at 3.

utilizing the market segmentation technique, a business can target its customers by establishing consumer profiles based on customer information, including demographics, past purchaser behavior, etc.[44] Boosted by the proliferation of e-commerce, target marketing practices have resulted in a tremendous amount of unsolicited e-mails being sent to potential customers.

From the viewpoint of the seller, consumer information is a necessary source for screening and selecting target customers, thus improving profit. Furthermore, consumer information may also be utilized to serve customer needs better and improve shopping convenience.[45] However on the consumer side, this information is considered private and should be protected from uncontrolled dissemination. This is especially important because consumer information collected for maintaining profiles may include nearly every aspect of an individual's life, ranging from basic demographics to confidential credit card information.[46]

Consumers are also seriously concerned that their personal information can not recover its confidentiality once it is made public and shared among businesses. One way to re-establish confidentially is to change this personal information. However while artificially created personal information may be easily changed and reset, biological demographics can not be altered to protect the right to privacy.[47]

---

[44] *Id.*

[45] David J. Klein, *Comment: Keeping Business Out Of The Bedroom: Protecting Personal Privacy Interests From The Retail World,* 15 J. MARSHALL J. COMPUTER & INFO. L. 391, 393 (1997).

[46] *Id.*, at 391.

[47] *Id*. at 393.

Another passive way to regain the confidentiality of consumer personal information is for consumers to ask businesses to remove this information from marketing lists,[48] but this act is not considered sufficient to protect consumer information from being transferred to other businesses.[49] In order to remove their personal information from the personality profiles, the consumers must identify the company to whom they initially provided their personal information and then request their profiles to be deleted.[50] However, if the initial list creator has already sold the information to other businesses, the consumers would be still faced with loss of privacy.

3. Classification of Consumer Information

Consumer information is made up of a variety of dimensions, because every fact about a consumer may be manipulated to generate meaningful information with respect to marketing. As previously discussed, businesses have utilized consumer information to target their markets, which can be done through market segmentation.[51] Accordingly, marketing scholars have attempted to classify consumer information to derive variables of market segmentation.[52]

---

[48] *Id.* at 397.

[49] *See*, R.J. Ignelzi, *Mail and Telejunk U.S. Marketers Have Your Number, Your Age and Shoe Size, Too*, S. D. Union-Trib., July 4, 1995, at E1.

[50] *See*, Nora Carrera, *One Man's Junk Is Another's Mail*, Rocky Mountain News (Denver, Co.), Sept. 25, 1995, at 38A.

[51] MICHAEL R. SOLOMON & ELNORA, W. STUART, *supra* note 10, at 202 ("Market segmentation is the process of dividing a larger market into smaller pieces based on or more meaningful, shared characteristics.").

[52] *See*, MICHAEL R. SOLOMON & ELNORA W. STUART *supra* note 10 at 202; *see* also LEON G. SCHIFFMAN & LESLIE LAZAR KANUK, CONSUMER BEHAVIOR 37 (7th ed. 2000).

This classification has been made in different dimensions. Some scholars provide 'broad' dimensions to classify consumer information,[53] while others offer 'specific' dimensions.[54] Although the dimensions for classification of consumer information are too diverse to be standardized, it is possible to derive several most common dimensions. Among other things, consumer demographics may be a dimension for classifying information. In addition, transaction-related data (e.g., amounts spent, buying habits, etc.) can be another dimension to be used.

Although classification of consumer information may be conducted from a variety of existing perspectives, it is necessary to establish a new dimension, which will be utilized for the legal analysis of protection of consumer information. This new dimension should be able to reflect the need for consumer information to be protected from illegal collection, use and dissemination. In other words, the degree to which consumers consider it to be important to protect their personal information should be reflected to the types of consumer information.

For example, personal information regarding financial data, including credit card, checking account and pin numbers is likely to be among the most confidentially treated private information whose collection or dissemination without proper authorization will result in committing a crime. On the other hand, information such as name and gender[55] may not draw critical attention from consumers, because this personal data can be available

---

[53] MICHAEL R. SOLOMON & ELNORA W. STUART, *supra* note 10, at 203-9 (providing three dimensions including demographics, psychographics, and behavior); WARD HANSON, PRINCIPLES OF INTERNET MARKETING 383 (2000) (suggested four dimensions including descriptive data, transaction history, preference measures and trigger events).

[54] *See, e.g.*, RAFI A. MOHAMMED, ROBERT J. FISHER, BERNARD J. JAWORSKI & AILEEN M. CAHILL, INTERNET MARKETING 89-90 (2002); LEON G. SCHIFFMAN & LESLIE LAZAR KANUK, *supra* note 52, at 37.

[55] *See*, WARD HANSON, *supra* note 53, at 383.

though telephone directories if the customer opts for publication with the local telephone company.

Another category of consumer information may be found in the psychological motivation of privacy, which can be positioned between the two extremes on the spectrum of privacy needs. A typical example of psychologically motivated privacy concerns may be related to protecting information on customer lifestyles and purchase behaviors.[56] The degree of motivation to protect this category of consumer information should vary depending on each consumer's personality; some are very sensitive to dissemination, while others are not.

These three categories mentioned above may be described as 'absolute', 'contingent', and 'negligible' with respect to the need for privacy protection.

4. Management of Consumer Information

Personal information collected from customers should be updated and sometimes discarded in order to make the consumer profile list meaningful for marketing activities.[57] For each stage of the profile management, customers have been sensitive to the privacy of their personal information.[58] For the collection stage, customers may be relieved of their

[56] *See*, LEON G. SCHIFFMAN & LESLIE LAZAR KANUK, *supra* note 52, at 37.

[57] The management process of consumer information to be utilized for marketing activities can be partitioned as collection, maintenance, and discard. In the collection stage, consumer information may be initially gathered and stored into a database. During the maintenance stage, consumers' personal information may be updated and changed. Finally, consumers' personal data may be discarded when they are outdated and useless.

[58] *See*, WARD HANSON, *supra* note 53, at 418.

concern for privacy by the introduction of privacy statements[59] intended to clarify the purpose of the information and its utility.[60]

For the maintenance stage, customers may be most concerned with unintended dissemination of their personal information. In this stage, businesses may release personal customer information in breach of privacy statements they gave to the individual consumers, in which case the customers should be legally protected and able to claim personal damages. Another example of unauthorized dissemination could occur if the security system of a company's consumer profile database is attacked by an outside hacker.

In discard, the final stage of consumer information, businesses may unload outdated consumer information from their consumer profile databases. Customers may be concerned when businesses do not completely erase the consumer profiles from the database, thus exposing the personal information to unknown or possibly malicious information collectors.

Not only businesses but the government seeks a vast amount of personal information that may be utilized for commercial activities.[61] Such information could cover personally sensitive profiles[62] and even a person's criminal history. The role of the government in managing consumer information should be different from that of businesses, in that the governmental purpose for maintaining personal information is to prevent fraudulent business

---

[59] *See, id.*, ("The privacy statements lay out the broad guidelines the site follows in handling information collected from individuals through Web use, surveys, purchases, or additional data sources merged and matched with online data.").

[60] *See, id.*

[61] David J. Klein, *supra* note 45, at 391.

[62] *Id.*

practices from being spread over consumers and industries, while businesses aim to utilize the information for commercial gains.[63]

Accordingly, the nature of management of consumer information is fundamentally different between the government and businesses. The government's main purpose of maintaining personal information should be to protect both consumers and industries. A separate legal consideration for governmental activities related to management of consumer information seems to be necessary to protect the public interest.

C. Consumer Privacy in E-Commerce

1.Backgrounds

Consumer information has been far more efficiently utilized since the introduction of e-commerce into the commercial arena. Although the functional role of consumer information in commercial activities (e.g., market segmentation) can be said to remain unchanged, the method of applying it to business has significantly shifted from paper-based to online-based, resulting in a tremendous reduction of time and costs in handling consumer data files.

In the meanwhile, consumers consider the collection of consumer information through the Internet as somewhat more risky than efficient. It seems consumers have not been so much enjoying the efficiencies of e-commerce as concerned about the protection of their personal information while being engaged in online commercial activities.[64] If untreated, such

[63] *See*, Mozelle W. Thompson, *supra* note 1, at 3-4.
[64] *See*, Omar Saleem, *supra* note 32, at 172.

concerns from consumers will eventually deteriorate e-commerce and at worst may eradicate the advantages of online transactions.[65]

To alleviate consumers' privacy concerns on the Internet, the government and industries may play their roles in different ways. The government can lessen privacy concerns by regulating business practices in managing customer personal information (e.g., FTC regulation).[66] However, the government's role in protecting consumer information has been criticized as inefficient.[67] Instead, it was suggested by the Federal Trade Commissions that consumer privacy in e-commerce will be more adequately protected if businesses regulate themselves (i.e. self-regulate).[68]

Although the government's regulation may be negatively influential to the industries by shrinking commercial activities, it is undeniable that there should at a minimum be legally enforceable measures by which unfair practices in the management of consumer information can be controlled. Thus, to foster the growth of e-commerce, it would be necessary for both the government and businesses to seek protection of consumer information.

2. Legal Characteristics

It is questionable whether traditional legal principles on privacy are applicable to today's privacy concerns on the Internet,[69] because newly raised online legal issues (e.g., online security, online jurisdictions, etc.) should be reflected in different perspectives. However, the

---

[65] *Id*. at 173.
[66] Debra A. Valentine, *supra* note 40, at 403.
[67] Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877, 890 (2000).
[68] Omar Saleem, *supra* note 32, at 174.
[69] *See*, *id.* at 176.

core concept of online privacy may still be the same as defined previously, except that the medium of information exchange has been changed to the Internet; online consumer privacy[70] can be defined as a legal right covering the consumer's control of his or her personal information on the Internet.

Because online privacy interests vary depending on types of information, types of personality traits and jurisdictions,[71] it would be impractical to sort out uniform legal principle applicable to all types of online privacy. First, it may be natural that financial information (e.g., credit card number, pin numbers, etc.) will draw more privacy concerns from the online customers than general demographic information does. Such variations in the degree to which consumers are concerned with online privacy will consequently be reflected in related regulations with respect to the intensity of indemnity for damages caused by violation of online consumer privacy.

Second, online consumer privacy may have to be protected for a specific group of consumers. For instance, the Children's Online Privacy Protection Act of 1998 (hereinafter "COPPA")[72] was enacted to protect online privacy for specific age groups. It would be inappropriate to apply uniform legal principles of online privacy to juveniles.

Finally, some jurisdictions may show keen interest in online consumer privacy and provide strict regulations while others do not. Such variation in online privacy interests may be significantly magnified across countries, affecting the intensity of regulation with respect

---

[70] In this thesis, the terms of E-commerce, online and the Internet, will be employed to denote the same meaning in the context of consumer privacy although they may have slight differences in their technical definitions.

[71] *See*, Dorothy Glancy, *Symposium At The Intersection of Visible and Invisible Worlds: United States Privacy and The Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH. L. J.357, 358 (2000).

[72] 15 U.S.C. §§ 6501-6506 (1999).

to online consumer privacy.[73] Cultural differences are likely to have some influence on consumer perceptions of online privacy. For instance, individualistic countries (e.g. the U.S.) are expected to be more responsive to the protection of online consumer privacy than collectivistic countries (e.g. Korea).

Consumers may experience violation of their online privacy rights in various ways. Several types of consumer concerns about information privacy have been reported.[74] One stream of consumer fears has been rooted in the threat of their personal information being tracked and collected "invisibly"[75] during interactions with online sellers. Such tracking systems have been known to be designed to identify online consumers' web surfing patterns and sometimes sneak into their hard drives.[76] The other stream of customer concerns is rooted in attacks by computer hackers on the confidential information stored in the online sellers' network systems.[77] For instance, customer credit card information may be accessed and copied without authorization, and the customers have been reportedly endangered by being asked to pay for unauthorized purchases.[78]

---

[73] *See*, Omar Saleem, *supra* note 32, at 178.

[74] Beth Givens, *Symposium on Internet Privacy: Privacy Expectations in a High Tech World*, 16 SANTA CLARA COMPUTER & HIGH TECH. L. J. 347, 352-4 (2000).

[75] *Id.*, at 352.

[76] *Id*.

[77] *Id.*, at 353.

[78] Elinor Mills Abreu, *FBI probing theft of 8 million credit card numbers*, AOL BUSINESS NEWS, Feb. 19, 2003, *at* http://my.aol.com (last visited Mar. 6, 2003).

Violations of consumer online privacy may be diagnosed by having guidelines to ensure fair information practices. Those guidelines have been provided by several authorities (including the UN,[79] OECD,[80] EU[81] and the FTC).[82]

On the whole, most of the guidelines suggested seem to have some common features among the authorities, which may be exemplified by the safe harbor principles.[83] With the advise of the European Commission, the U.S. Department of Commerce developed the safe harbor principles with a view towards narrowing the gap of privacy protection policies between the two authorities and preparing "a streamlined means for U.S. organizations to comply with the EU Directive".[84]

Included in the safe harbor principles are notice, choice, onward transfer, security, data integrity, access, and enforcement.[85] Each of these principles may be utilized as a criterion to evaluate the protection by business of online consumer privacy, while also functioning as a legal framework for classification of the violations.

---

[79] United Nations (UN), Guidelines Concerning Computerized Personal Data Files (1990), *at* http://europa.eu.int/ comm/ internal_market/ en/ dataprot/ inter/ un.htm (last visited Mar.9, 2003).

[80] Organization for Economic Cooperation and Development (OECD), Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980), *at* http://europa.eu.int/ comm/ internal_market/ en/ dataprot/ inter/ priv.htm (last visited Mar. 9, 2003).

[81] EU Council of Europe, Recommendation No R (99) 5 of the Committee of Ministries to Member states for the Protection of Privacy on the Internet (1999), *at* http://www.coe.fr/ cm/ ta/ rec/ 1999/ 99r5.htm (last visited Mar. 9, 2003).

[82] Federal Trade Commission (FTC), Privacy Online: A Report To Congress (1998), *at* http://www.ftc.gov/ reports/ privacy3/ toc.htm (last visited Mar. 9, 2003).

[83] U.S. Department of Commerce, Safe Harbor Privacy Principles (2000), *at* http://www.export.gov/ safeharbor/ SHPRINCIPLESFINAL.htm (last visited Mar. 9, 2003) (With the advisement of the European Commission, the U.S. Department of Commerce developed the safe harbor principles "in order to bridge these different privacy approaches and provide a streamlined means for U.S. organizations to comply with the EU Directive").

[84] U.S. Department of Commerce, Safe Harbor Overview, *at* http://www.export.gov/ safeharbor/ sh_overview.html (last visited Mar. 9, 2003).

[85] *See*, U.S. Department of Commerce, *supra* note 83.

CHAPTER 3

RELATED REGULATIONS IN THE U.S. AND KOREA

A. The U.S.

1. Legal Characteristics

Protection of consumer online privacy in the U.S. tends to rely more on self-regulatory measures than on governmental controls[86], and to be "sectoral"[87] in its statutory regulations. Businesses have voluntarily propelled themselves to protect customer online privacy with the goal of avoiding the government's administrative regulation and legislation.[88] While studies on the pervasiveness of online collection, sharing and sale of personal data[89] have motivated the need for state or federal regulations regarding the Internet consumer privacy, it was also reported that governmental authorities should leave industries to be self-regulated, because governmental intervention may distort the market function which would otherwise

---

[86] Jordan M. Blanke, *"Safe Harbor" and the European Union's Directive on Data Protection*, 11 ALB. L. J. SCI. & TECH. 57, 69 (2000).

[87] Beth Givens, *supra* note 74, at 348.

[88] Jordan M. Blanke, *supra* note 86, at 69.

[89] Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace (May 2000), *at* http://www.ftc.gov/ reports/ privacy2000/ privacy2000text.pdf (last visited Mar. 10, 2003).

eventually lead industries to comply with consumers concerns with online privacy in order to survive in the market system.[90]

In addition to the 'self-regulatory' characteristic, the 'sectoral approach' has characterized the United States' regulation of industry practices with respect to customer online privacy,[91] meaning that the U.S. regulations on privacy are industry-specific; thus, each section of industries has its own statutory regulations. Most of the regulations are intended to be applied to public organizations, while only a few laws have been enacted to control private institutions.[92]

Several negative effects of the sectoral approach were suggested by an opponent of sectoral regulation. First, consumers have been bewildered over which regulatory rules may be applied to their particular cases, because there are no easy and common rules on privacy protection.[93] Second, it has long been recognized by industries that they can normally collect consumer data without permission due to the "patchwork"[94] type of regulations on consumer privacy.[95]

In the U.S., the FTC is a major federal authority in charge of consumer protection issues, several of which may be exemplified by online consumer privacy,[96] unfair methods of competition[97] and unfair acts or practices.[98] Rather than legislating online consumer

---

[90] William S. Challis & Ann Cavoukian, *The Case for A U.S. Privacy Commissioner: A Canadian Commissioner's Perspective*, 19 J. MARSHALL J. COMPUTER & INFO. L. 1, 4 (2000).

[91] Beth Givens, *supra* note 74, at 348.

[92] Jordan M. Blanke, *supra* note 86, at 66.

[93] *See*, Beth Givens, *supra* note 74, at 349.

[94] *Id.*

[95] *Id.*, at 350.

[96] *See*, *supra* note 89, at 1-64.

[97] 15 U.S.C. § 45 (a) (1) (2000).

[98] *Id.*

protection measures, the U.S. regulatory authorities (i.e. the FTC and state agencies) have coped with conflicts between businesses and consumers by way of applying previously existing laws to the Internet cases.[99]

A unique point was suggested with respect to the United States' regulation of online privacy that it is not rooted in protection of human rights but in protection of the commercial interest vested in consumer personal data, because the regulatory powers are given to the FTC.[100] While the FTC aims to protect consumer online privacy rights, it has also been favorable to the self-regulatory efforts of industries and encouraged them to enhance consumer data privacy, arguing that:

> The Commission believes that self-regulation is the least intrusive and most efficient means to ensure fair information practices online, given the rapidly evolving nature of the Internet and computer technology.[101]

Partial and indirect roles in regulating Internet privacy are played by other federal authorities, including the Federal Communication Commission (hereinafter 'FCC')[102] and the Department of Commerce.[103] If a written notice of civil action brought against any person's violation of privacy by the State is delivered to the Commission, the FCC is authorized "to intervene in the action, to be heard on all matters arising therein, and to file petitions for appeal."[104]

---

[99] Michael Cordera, *NOTE AND COMMENT: E-Consumer Protection: A Comparative Analysis of EU and US Consumer Protection on the Internet*, 27 RUTGERS COMPUTER & TECH. L. J. 231, 252 (2001).

[100] Omar Saleem, *supra* note 32, at 179.

[101] Federal Trade Commission Report, Self-Regulation and Privacy Online, *at* http://www.ftc.gov/ os/ 1999/ 9907/ pt071399.htm (last visited Mar. 11, 2003).

[102] 47 U.S.C. § 227 (c), (f) (2000).

[103] *See*, U.S. Department of Commerce, *supra* note 84.

[104] 47 U.S.C. § 227 (f) (2000).

The Department of Commerce has been attempting to adjust the differences in privacy regulations among countries. For instance, the safe harbor principles drafted by the Department of Commerce[105] were proposed to modify the gap between the U.S. and EU regarding regulatory practices on Internet privacy. The role of the Department of Commerce in carrying out the safe harbor principles may be said as indirect, because most of the practical matters (e.g., enforcement) with respect to the principles have been administered by the FTC.[106]

2. Related Regulations

The FTC's Fair Information Practices

Referring to the OECD guidelines and EU directives, the FTC suggested "five core principles of privacy protection"[107], which were called "fair information practices".[108] The FTC reported that while most of the Internet-based businesses collected personal information from customers, they were not prepared with proper measures to protect consumer online privacy, which should include appropriate notice of their information practices and privacy policies.[109]

The principles of fair information practices consist of : (1) Notice/Awareness; (2) Choice/Consent; (3) Access/Participation; (4) Integrity/Security; and (5)

---

[105] *See*, U.S. Department of Commerce, *supra* note 84.

[106] *Id.*

[107] Federal Trade Commission, Privacy Online: A Report to Congress, at 7-11 (1998), *available at* http://www.ftc.gov/ reports/ privacy3/ fairinfo.htm (last visited Mar. 12, 2003).

[108] *Id.*, at 7

[109] *Id.*, at 40.

Enforcement/Redress.[110] Among the five principles, notice was recognized as the most critical, requiring that a proper notice should be given to consumers before a business gathers personal information.[111] The FTC attempted to clarify the contents of notice made by businesses, suggesting that the six common elements derived from the OECD Guidelines and the EU Directive should be included in the online privacy notice.[112] Furthermore, the FTC required that an Internet business disclose its information practice in a prominent portion of its Web page.[113]

Choice was described as "the second widely accepted principle of fair information practice."[114] This principle requires that consumers be given at least some chances to decide whether their personal information is allowed to be used and disseminated by the businesses, which can be realized by opt-in and opt-out provisions inserted in the disclosure of online privacy.[115] While it may be realistically difficult for the customers to avoid a business collecting and manipulating consumer information,[116] the choice principle is apparently expected to serve an important rule in limiting the unbound management of consumer data.

The third principle, access, denotes that customers' personal information stored in a business databases should be easily available so that customers can check and confirm data accuracy and completeness.[117] Several specific requirements applying to this principle

---

[110] *Id*, at 7.
[111] *Id*.
[112] *Id*. at 7-8 (The six basic elements of notice include identification of data collector, use of data, potential recipient, nature of data/collecting methods, obligation of data submission, and data protection policy).
[113] *Id*., at 8.
[114] *Id*.
[115] *Id*., at 9.
[116] David J. Klein, *supra* note 45, at 406.
[117] Federal Trade Commission, *supra* note 107, at 9.

include "timely and inexpensive access to data, a mechanism by which the data collector can verify the information, and the means by which corrections and/or consumer objections can be added to the data file and sent to all data recipients."[118]

The integrity/security principle requires that data should be accurate and safe from unauthorized access.[119] While the notion of integrity seems to somewhat overlap with the access principle (in that integrity demands consumer accessibility to data files to ensure the accuracy of data), the FTC suggests that the collectors should only use reputable sources of information and discard outdated data to enhance integrity.[120] According to the security principle, consumer data are required to be protected against "loss and the unauthorized access, destruction, use, or disclosure of the data".[121]

Enforcement/Redress is recognized as an essential part of fair information practices, because it is generally understood that, without an enforcement and redress mechanism, fair information principles may be only "suggestive rather than prescriptive"[122] and play limited roles in protecting online consumer profiles. The FTC provided three alternative approaches by which fair information principles can be enforced and redressed, including "industry self-regulation, legislation that would create private remedies for consumers, and/or regulatory schemes enforceable through civil and criminal sanctions."[123]

---

[118] *Id.*
[119] *Id.*, at 10.
[120] *Id.*
[121] *Id.*
[122] *Id.*
[123] *Id.*

Safe Harbor Principles (the U.S. Department of Commerce)

The U.S. safe harbor principles have been in operation for two years since the final documents were made public in 2000.[124] The United States' efforts to develop the safe harbor principles were propelled by the European Union's comprehensive privacy legislation, the Directive on Data Protection (hereinafter "the Directive")[125], which was activated on October 25, 1998.[126] The Directive stipulates:

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.[127]

In response to the EU directives on personal information, the U.S. Department of Commerce attempted to establish guidelines that were as comparable as possible with the EU directives and could be voluntarily adopted by US organizations, which resulted in the seven safe harbor principles.[128] In July 2000, the safe harbor principles proposed by the U.S. were unanimously approved by the European Union Member States and went into effect.[129]

While a U.S. organization may voluntarily choose to be subject to the safe harbor principles, once it became a safe harbor member, it must comply with them to protect

---

[124] U.S. Department of Commerce, *supra* note 83.

[125] EUR-Lex: Community Legislation in Force, Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L281) 31 (November 23, 1995), *available at* http://www.lexis.com (last visited Mar. 15, 2003).

[126] U.S. Department of Commerce, *supra* note 83.

[127] EUR-Lex: Community Legislation in Force, *supra* note 125, art.25.1.

[128] *See*, U.S. Department of Commerce, *supra* note 83.

[129] U.S. Department of Commerce, Introductory Welcome Statement, *at* http://www. export.gov/ safeharbor (last visited Mar. 15, 2003).

personal data and information transmitted from a European Country.[130] These principles[131] include notice, choice, onward transfer, security, data integrity, access, and enforcement, and therefore have much in common with the FTC's fair information practices[132] except for onward transfer. In relation to onward transfer, it is stipulated that:

> Where an organization wishes to transfer information to a third party that is acting as an agent, it may do so if it first either ascertains that the third party subscribes to the Principles or is subject to the Directive or another adequacy finding or enters into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant Principles.[133]

According to the onward principle, an organization is allowed to disclose personal information to a third party that is working for the organization as an agent only if the third party maintains "at least the same level of privacy protection as is required by the Principles."[134]

Congressional Legislation

Congressional legislative activities on protection of personal information have been widely known as the sectoral approach, focusing the legislative goal on specific industries.[135] In addition, U.S. privacy laws have been enacted to respond to changes and new developments in technologies regarding collecting personal information and its uses.[136] Most

---

[130] U.S. Department of Commerce, *supra* note 126.
[131] *Id.*
[132] Federal Trade Commission, *supra* note 107, at 7.
[133] EUR-Lex: Community Legislation in Force, *supra* note 125.
[134] *Id.*
[135] Debra A. Valentine, *supra* note 66, at 404.
[136] *E.g.*, Privacy Act, 5 U.S.C. § 552 (1994); Fair Credit Reporting Act, 15 U.S.C. §§ 1681-1688t (1994); Freedom of Information Act, 5 U.S.C. § 552 (2000); Video Privacy Protection Act, 42 U.S.C. § 2000aa (2000).

of the patchwork legislation was reported to have defects in three aspects: "new and unanticipated uses of digital data (i.e., other than the purposes for which it was originally collected); the inconsistent application of similar privacy rules by different record keepers; and, most significantly, the lack of effectiveness in oversight and uniform enforcement"[137], which have been the major sources of consumer pessimism concerning legislative efforts to protect online privacy rights.[138]

The U.S. legislation on protection of privacy rights can be classified into two categories based on the type of the main entities collecting, managing and releasing personal information: the governmental organizations covering federal and state levels, and private industries. A notable example of privacy legislation regulating the government's use of information[139] may be the Freedom of Information Act[140] (hereinafter "FOIA"), which was codified to allow public access to government agency records. In *HMG Marketing Association v. Freeman*, the main purpose of the FOIA was interpreted as enhancing individuals' rights to know about the government's activities.[141]

To limit individuals' right to know, the FOIA also provides nine exemptions by which the government agency is excused from permitting the public to have access to data files.[142] For example, a governmental agency may be exempted from disclosure of "trade secrets and

---

[137] William S. Challis & Ann Cavoukian, *supra* note 90, at 9.

[138] *Id*. at 10.

[139] 18 U.S.C. §§ 2510-2511, § 2701 (1994) (included in this category is the Electronic Communications Privacy Act, which regulates the federal and state governments' access to oral, wire, and electronic communications).

[140] 5 U.S.C. § 552 (2000).

[141] 523 F. Supp. 11, 13 (S.D.N.Y. 1980).

[142] 5 U.S.C. § 552 (b) (2000).

commercial or financial information obtained from a person and privileged or confidential."[143]

Another example of Congressional legislation to protect personal information from governmental misuse can be found in the Tax Reform Act of 1976, which was enacted to assure the confidentiality of information collected through the tax return process and limit the dissemination of the related personal tax return information.[144]

The other stream of legislation to protect consumer privacy from abusive practices in the industry[145] may be exemplified by the Fair Credit Reporting Act of 1970(hereinafter "FCRA").[146] The FCRA was enacted to assure that consumer credit reporting agencies adopt reasonable procedures to improve the confidentiality, accuracy, and relevancy of consumer information.[147] Another piece of legislation in this stream would be represented by the Right to Financial Privacy Act[148] which aims "to protect customers of financial institutions from unwarranted intrusion into their records while at same time permitting legitimate law enforcement activity by requiring federal agencies to follow established procedures when seeking customer's financial records."[149]

---

[143] 5 U.S.C. § 552 (b) (4) (2000).

[144] 26 U.S.C. § 6103 (1994).

[145] Included in this category are the Cable Communication Policy Act, 47 U.S.C. § 551 (a) (1994); Telemarketing Protection Act, 47 U.S.C. § 227 (1994); Video Privacy Protection Act, 18 U.S.C. §§ 2710-2711 (1994); Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (1994); and the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6510-6506 (2000).

[146] 15 U.S.C. §§ 1681-1681t (1994).

[147] 15 U.S.C. § 1681 (b) (1994).

[148] 12 U.S.C. §§ 3401-3422 (1994).

[149] 12 U.S.C. § 3401, (1994).

Attitudes of the Courts

Federal courts have taken a position pursuant to the FOIA that personal data stored in government agencies should be kept confidential from industries if the information is requested to be utilized for commercial purposes.[150] In order to apply Exemption 6 of the FOIA[151] in *HMG Marketing Associates v. Freeman*, the federal court focused on whether the plaintiff's effort to improve merchandising efficiency by use of a mailing list requested from the defendant reflected any public interest, concluding that the plaintiff's request would not serve to facilitate public interest, but rather foster the delivery of unsolicited junk mails to potential customers.[152]

While the FOIA was enacted to enhance public access to personal information collected by government agencies,[153] it seems to be an agreed viewpoint that federal courts have been more favorable to protection of personal information when personal data are requested for commercial use.[154] For instance, in *Wine Hobby USA, Inc. v. United States IRS*, the federal court stressed that "the disclosure of names of potential customers for commercial business is wholly unrelated to the purposes behind the Freedom of Information Act and was never contemplated by Congress in enacting the Act."[155]

---

[150] *See, e.g.*, Minnis v. United States Dep't of Agriculture, 737 F.2d 784, 787 (9th Cir. 1984) (concluding that, "absent any asserted public interest in disclosure, a commercial interest would not justify the invasion of privacy."); *see also* 523 F. Supp. at 14 (S.D.N.Y. 1980) (concluding that "the disclosure requested by the marketer would have been a clearly unwarranted invasion of personal privacy.).

[151] 5 U.S.C. § 552 (b) (6) (2000).

[152] 523 F. Supp. at 14 (S.D.N.Y. 1980).

[153] *Id.*, at 141.

[154] *See*, David J. Klein, *supra* note 45, at 400.

[155] 502 F.2d 133, 137 (3rd Cir. 1974).

In contrast to the federal court jurisdiction over government agency control of personal data, state courts are in charge of legal actions brought against industries for disclosure of customer data.[156] In an evaluation of invasion of privacy, an Illinois appellate court revealed that four branches of the privacy invasion tort founded on the Restatement (Second) of Torts[157] can be applied to investigate the defendant's violation of privacy rights, including "(1) an unreasonable intrusion upon the seclusion of another; (2) an appropriation of another's name or likeness; (3) a public disclosure of private facts; and (4) publicity which reasonably places another in a false light before the public."[158]

It seems to be evident that state courts apply the common law of torts to protection of personal information from commercial exploitation;[159] while federal courts rely on Congressional legislation for protection of privacy rights.[160] Although the Restatement (Second) of Torts[161] was intended to protect personal privacy rights, state courts have been rather conservative in its interpretation.[162] For example, in *Dwyer v. American Express Co.*, the state court rejected the alleged violations of the right to privacy, holding that the trial court's decision should not be reversed because the defendant's release of voluntarily submitted personal information to third parties was neither impermissible nor detrimental to the cardholders in a meaningful way.[163]

---

[156] *See, e.g.*, Dwyer v. American Express Co., 652 N.E.2d 1351, 1353 (Ill. App. Ct. 1995).
[157] Restatement (Second) of Torts 652 (1977).
[158] 652 N.E.2d at 1353 (Ill. App. Ct. 1995).
[159] *See, id.*
[160] *See, e.g.*, 502 F.2d at 137 (3rd Cir. 1974).
[161] Restatement (Second) of Torts 652 (1977).
[162] *See*, David J. Klein, *supra* note 45, at 402.
[163] 652 N.E.2d at 1351 (Ill. App. Ct. 1995).

In response to the differences between federal and state court attitudes to commercial exploitation of personal information collected by government agencies and industries, it was argued that when individuals request to keep their personal information submitted to businesses from being released to third parties for commercial purposes, state courts should interpret the common laws more actively to prevent abusive commercial exploitation.[164] The amicable attitudes of the state courts toward protection of consumer privacy will lead e-consumers to be emancipated from the fears of violation of online privacy and help the emerging e-commerce to settle down as a new business paradigm.

B. Korea

1. Legal Characteristics

The world trend of introducing Internet technology into business operation has not been an exception in Korean industries,[165] which has equally endangered the Korean consumers with threats of uncontrolled dissemination of their personal information. When recently faced with consumer privacy concerns regarding personal information in cyberspace, the government of Korea actively attempted to enact new laws to regulate the handling of personal data collected by public agencies and private businesses.[166]

---

[164] David J. Klein, *supra* note 45, at 404.

[165] *See*, Korea Information Security Agency, Reports on Information Security Efforts by Selected Private Sectors: As for Year 2001, at 6 (2002).

[166] *See*, *e.g.*, Public Organization's Protection of Personal Information Act of 1994; Promotion of Information Networks and Protection of Personal Information Act of 2000, *available at* http://www. moleg. go.kr (last visited Mar 21, 2003).

Legislative activities in Korea to protect personal information from misuse and unauthorized access have been sectoral and restricted in specific privacy issues without a general law applicable to consumer privacy rights.[167] In Korea, the legal system for protection of personal information consists of two parts: public[168] and private sectors.[169] It has been suggested that a comprehensive law to protect privacy rights should be enacted to reduce individuals' confusion resulting from the fast-changing information technology in each field of industry.[170]

The Korean Constitution provides a fundamental legal basis for protection of individuals' privacy stipulating that "all of the people should not be disturbed for the freedom and secret of private life[171] and should not be hampered for the secret of their communications".[172] Both these constitutional privacy rights may be interpreted in two ways: exclusive and inclusive. Some lawyers interpret the constitutional privacy rights exclusively so that their applicability is restricted to only protection of personal rights[173], while others interpret them inclusively so that their applicability extends to protection of personal information as a property right.[174]

---

[167] *See*, Eun Woo Lee, *Legal Issues on Privacy and Protection of Personal Information*, Symposium Reports of Civil Activists Associates for Protection of Privacy 1, 1 (2001), *at* http://www. privacy.or.ke/ privacy.text.htm (last visited Mar. 21, 2003).

[168] *E.g.*, Public Organization's Protection of Personal Information Act of 1999; Public Organization's Disclosure of Information Act of 1996, *available at* http://www. moleg. go.kr (last visited Mar 21, 2003).

[169] *E.g.*, Act on Promotion of Information and Communications Network Utilization and Information Protection, of 2002; Framework Act on Informationalization Promotion of 2002; Protection of Communication Secrets Act of 2002, *available at* http://www.moleg. go.kr (last visited Mar. 21, 2003).

[170] Young Wha Jung, *Policy Measures for Protection of Privacy in Information Society*, Symposium Reports of Civil Activists Associates for Protection of Privacy 1, 12 (2001), *at* http://www. privacy.or.kr/ privacy.text.htm (last visited Mar. 21, 2003).

[171] KOREA CONST. art. 17.

[172] KOREA CONST. art. 18.

[173] *See, e.g.*, CHEOL SOO KIM, THE CONSTITUTION OF KOREA 260 (2000).

[174] *See, e.g.*, Young Wha Jung, *supra* note 170, at 14.

In order to accommodate the revolutionary changes in information technology, constitutional privacy rights should be interpreted inclusively.

The Ministry of Information and Communication is a major authority regulating the treatment of personal information by private industries; its power is based on the Act on Promotion of Information and Communications Network Utilization and Information Protection, and the Framework Act on Informationalization Promotion and the Protection of Communication Secrets Act.[175] On the other hand, the Ministry of Government Administration and Home Affairs is responsible for the protection of personal information stored in public organizations as authorized by the Public Organization's Protection of Personal Information Act and the Public Organization's Disclosure of Information Act.[176] Another regulatory authority to control the handling of confidential information is the Ministry of Finance and Economy based on the Use and Protection of Credit Information Act.[177]

Protection of consumer privacy in Korea has been dominated by government regulation, while self-regulation may be more effective in preventing violation of privacy rights.[178] It does not seem that businesses have attempted to organize themselves to provide guidelines

---

[175] *See*, Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection of 2001; Enforcement Decree of the Framework Act on Informationalization Promotion of 2002; Enforcement Decree of the Protection of Communication Secrets Act of 2002, *available at* http://www.moleg.go.kr (last visited Mar. 21, 2003).

[176] *See*, Enforcement Decree of the Public Organization's Protection of Personal Information Act of 1995; Enforcement Decree of the Public Organization's Disclosure of Information Act of 1996 (last revised in 1999), *available at* http://www.moleg.go.kr (last visited Mar. 21, 2003).

[177] *See*, Enforcement Decree of the Use and Protection of Credit Information Act of 1995, *available at* http://www.moleg.go.kr (last visited Mar. 21, 2003).

[178] *See*, Sun Kyung Kwun Comparative Analysis of Protection of Personal Information: the U.S. and Korea, *at* http://www.cyberprivacy.or.kr (last visited Mar. 21, 2003).

to protect their customer information. Considering the potential pervasiveness of Internet transactions, it would be understandable if consumer privacy could not be protected solely by governmental regulation, but rather should be balanced with industry self-regulation.

Although a "right to know" is not specified in the Constitution of Korea, several cases decided by the Constitutional Court of Korea have consistently confirmed that the right to know should be recognized as a quasi-constitutional right.[179] However, a right to know has been recognized with some restrictions[180] due to the constitutional right of individual privacy specified in the Korean Constitution.[181] The Court's attitude toward personal information has been more favorable towards protection of privacy rights than promotion of the right to know for the public.[182]

2. Related Regulations

The Public Organization's Disclosure of Information Act

The Public Organization's Disclosure of Information Act (hereinafter "PODIA") was legislated to guarantee people's right to know and promote the transparency of government activities and people's participation in administration.[183] The PODIA is applicable only to government organizations,[184] including all agencies pertaining to the Administration, the

---

[179] Korea Constitutional Court, 88 Hunma 22 (September 4, 1989); Korea Constitutional Court, 90 Hunma 133 (May 13, 1991); Korea Constitutional Court, 93 Hunma 174 (August 31, 1994); Korea Constitutional Court, 92 Hunba 31 (December 29, 1994).

[180] *See*, Public Organization's Disclosure of Information Act of 1996, art.7, *at* http://www.moleg.go.kr (last visited Mar. 22, 2002).

[181] KOREA CONST. art. 17.

[182] Appellate Court of Korea, 94ku39262 (1995).

[183] Public Organization's Disclosure of Information Act of 1996, art. 1.

[184] *Id.*, art. 4, cl. 1.

National Assembly, and the Judicial Department, as well as local governments and others designated by the President.[185]

The PODIA specifies several types of information that are not subject to the request of disclosure, including information designated to be kept confidential by other laws, information potentially harmful to public safety and national interest when publicized, information being utilized in ongoing adjudication, personal information that is individually identifiable, etc.[186] Accordingly, the government agencies will be liable to disclose to the public such information that is not applicable to Article 7 of the PODIA.

Those who can claim information from public organizations include natural persons, legal persons, and foreigners.[187] The disclosure of information made by public organizations is strictly regulated by the PODIA so that the autonomy is hardly bestowed to each public organizations; thus, the ranges and methods of disclosure are very inflexible.[188] The PODIA may be quoted to protect personal information passively, because its main legislative purpose is to promote the right to know for the public.

The Public Organization's Protection of Personal Information Act

The legislative purposes of the Public Organization's Protection of Personal Information Act (hereinafter "POPPIA") are to protect personal information being processed through computer operations and to help the government agencies to perform public affairs

[185] *Id*., art. 2, item 3.
[186] *Id*., art. 7.
[187] *Id*., art. 6.
[188] *See*, Young Wha Jung, *supra* note 170, at 17.

properly.[189] Personal information is defined as information that may be individually identifiable through personal cues such as the civil registration number[190] and name contained in it.[191] The POPPIA has been quite inclusively protecting personal information by stipulating that information not containing personal identification cues will still be considered as being individually identifiable if an individual is identifiable through its combination of other information.[192]

According to the POPPIA, the chief officer of a public organization should take appropriate measures to prevent theft, divulgence and forgery of personal information collected, and should make every efforts to keep it accurate and updated.[193] The POPPIA stipulates that the chief officer may provide the collected personal information to other organization only in accordance with relevant laws;[194] thus an arbitrary dissemination of personal information is strictly prohibited. The information manager of a public organization is obliged to keep personal information stored in the database from being divulged, processed without proper authorization, or utilized for wrongful purposes.[195]

The POPPIA specifies that the chief officer of a governmental organization should allow an individual to inspect his or her personal information stored in the data files with regard to its accuracy and should take a proper measure to make a correction if the collected information is erroneous and defective.[196] The bestowal of the inspection right to individuals

---

[189] Public Organization's Protection of Personal Information Act, art. 1.
[190] This can be said to be equivalent of the U.S. social security number.
[191] Public Organization's Protection of Personal Information Act, art. 2, item 2.
[192] *Id.*
[193] *Id.*, art. 9.
[194] *Id.*, art. 10.
[195] *Id.*, art. 11.
[196] *Id.*, art. 12.

is expected to reinforce the accuracy of personal information collected and processed by the government organizations.

The Act on Promotion of Information and Communications Network Utilization and Information Protection

The Act on Promotion of Information and Communications Network Utilization and Information Protection (hereinafter "APICNUIP") aims to protect personal information from unauthorized disclosure when individuals utilize communication services, thus promoting public welfare through formation of an environment in which the information and communication network can be used safely.[197] In addition, the APICNUIP is enacted to protect privacy among individuals, which may be distinguished from the two acts[198] described previously in that it regulates violation of privacy by private entities.

The APICNUIP defines personal information as data that are individually identifiable images, symbols, characters and sounds combined with name and citizen registration numbers.[199] This is substantially the equivalent of the definition of personal information made in the POPPIA, except that personal information in the APICNUIP is more specifically

[197] Act on Promotion of Information and Communications Network Utilization and Information Protection, art. 1.

[198] Public Organization's Disclosure of Information Act; The Public Organization's Protection of Personal Information Act.

[199] Act on Promotion of Information and Communications Network Utilization and Information Protection, art. 2, item 6.

described than it is in the POPPIA.[200] Such difference indicates that the APICNUIP is more oriented toward protection of Internet privacy than is the POPPIA.

The APICNUIP was enacted as a special law to the Civil Code with respect to indemnity for mental and financial damages.[201] The enactment of the APICNUIP has made it easier for the claimant to be indemnified for the damage caused by violation of privacy, because it reduces the claimant's burden in having to prove the counterpart's willfulness and negligence, which are fundamental requirements for torts in the Civil Code.[202]

Chapter 4 of the APICNUIP[203] contains stipulations about the protection of personal information collected by information and communication service providers[204] with respect to legal issues including collection,[205] use and dissemination.[206] The APICNUIP specifies that in order to collect personal information, the service providers should obtain consents from the individuals.[207] Such personal information includes not only objective (e.g., date of birth, citizen registration number) but also subjective personal data including religious belief, medical history, ideology, etc.[208]

---

[200] *See*, Public Organization's Protection of Personal Information Act, art 2, item 2.

[201] Korea Civil Code, art. 750.

[202] *Id.*

[203] Act on Promotion of Information and Communications Network Utilization and Information Protection, art. 22-40.

[204] The scope of information and communication service providers is specified in article 2 of the APICNUIP and includes business entities that provide or intermediate information using electric communication services offered by the electric communication businesses. For definition of the electronic communication businesses, see article 2 of the Electric Communications Business Act, *available at* http://www.moleg.go.kr, (last visited Mar. 22, 2002).

[205] Act on Promotion of Information and Communications Network Utilization and Information Protection, art. 22-23.

[206] *Id.*, art. 24-29.

[207] *Id.*, art. 22, cl.1.

[208] *Id.*, art. 23.

Regarding the use and dissemination of personal information, the APICNUIP stipulates that the service providers should neither use nor disseminate personal information without consent of the individuals except in three cases: calculation of service fees, statistically analyzed data that are not individually identifiable, and designation by other laws.[209]

Other Regulations

In addition to the regulations previously described related to the protection of personal information, two more acts to promote privacy rights are found in the Korean regulatory system.

First, the Protection of Communication Secrets Act (hereinafter "PCSA") was legislated to protect communication secrets and promote freedom of communication, ensuring that a legitimate process should be followed when restrictions may be placed on the freedom of communication.[210] According to the PCSA, nobody is allowed to read the letters of others, inspect electric communication, or record conversations among others that are not open to the public.[211] However, the PCSA stipulates several exceptions allowing government agencies to interfere with personal communications, including potential threats to national security[212] and states of emergency.[213] The PCSA may be distinguished from other privacy regulations in that it mainly protects the confidentiality of messages flowing from one individual to another, while others regulate the collection, management and dissemination

[209] *Id.*, art. 24, cl.1.
[210] Protection of Communication Secrets Act of 2002, art. 1., *available at* http:// www.moleg.go.kr (last visited Mar. 21, 2003).
[211] *Id.*, art. 2, cl. 1.
[212] *Id.*, art. 7.
[213] *Id.*, art. 8.

of personal data. Another regulation to protect personal information may be found in the Use and Protection of Credit Information Act[214] (hereinafter "UPCIA"). The UPCIA aims to properly protect the confidentiality of an entity's financial standing from misuse by the evaluators of credit information and to promote the systematic management of credit information and its efficiency.[215]

In relation to the collection of personal credit information, the UPCIA stipulates that the service providers of credit information should not collect or investigate personal information about religious belief, political ideology or other private lifestyles;[216] in addition, credit information collected should be accurate and precise.[217] In order to protect individuals from violations of privacy, the UPCIA requires that credit information including medical history, individually identifiable profiles (e.g., name, citizen registration number, address, etc.) and other personal credit information designated by the presidential decree should be disseminated by the service providers only with notification of the dissemination to the individuals concerned.[218]

Attitude of the Courts

The courts seem to have been favorable to protection of personal information. For instance, the Supreme Court of Korea rejected a claim to force the disclosure of personal information including age, name and financial status, stating that it may violate the rights of

[214] Use and Protection of Credit Information Act of 2002, *available at* http://www. moleg.go.kr, (last visited Mar. 20, 2003).
[215] *Id.*, art. 1.
[216] *Id.*, art. 15, cl.1, item 3.
[217] *Id.*, art. 15, cl.1, item 4.
[218] *Id.*, art. 15.

privacy and freedom.[219] In another reported case in favor of personal privacy, the appellate court held that the rights of privacy and freedom should be given higher priority than the right to know, because privacy rights are more specifically and immediately influential to the protection of individual rights while the right to know is indirect and general.[220]

In contrast to the courts' amicable attitudes toward protection of personal information introduced thus far, several cases did not recognize the right to protect personal information. For instance, the Supreme Court of Korea held that names, addresses and telephone numbers acquired from the alumni directory do not pertain to personal credit information defined by the UPCIA[221] because they do not provide any information on the financial status of individuals; thus it wold not be illegal to collect personal information through an alumni directory.[222]

Another decision by the administrative court of Korea which was negative to the protection of personal information indicates that such information being utilized for trial may be disclosed if it does not have any impact on the court's decision.[223] Notably, when they deny the right to protect personal information, Korean courts have not been relying on an abstract reason such as right to know, but specific reasons as shown in the previous examples.

---

[219] For details, *see*, Supreme Court of Korea, 96noo2439 (May 23, 1997).
[220] For details, *see*, Appellate Court of Korea, 94Ku39262 (Aug. 24, 1995).
[221] The Use and Protection of Credit Information Act art. 23.
[222] The Supreme Court of Korea, Sunko99do6 (July 28, 2000).
[223] The Administrative Court of Korea, 98Ku3692 (Feb. 25, 1999).

C. Comparisons

Regulatory practices with respect to protection of personal information have been investigated in the U.S. and Korea, with the major focus being put on the regulatory authorities, legislative actions, and judicial decisions of each country. This section will comparatively analyze the regulatory practices of the two countries.

1. Regulatory Authorities

As found in Chapter 3,[224] in the U.S., the FTC, Department of Commerce and state agencies are the major authorities in charge of protecting consumer privacy, while in Korea the agencies are the Ministry of Information and Communication, Ministry of Government Administration and Home Affairs and Ministry of Finance and Economy. The regulatory practices of both countries have in common that the regulatory agencies are under direct control by the administrative power. However, the way that the regulatory authorities exert their power has been shown to be different in that the U.S. authorities put more emphasis on self-regulation, while the Korean authorities directly control business practices with respect to the protection of personal information.[225]

Due to the duality of the U.S. political and legal systems (i.e., federal and state levels), a uniform regulation across the nation seems to be difficult to achieve.[226] In Korea, however,

---

[224] *See*, U.S. Department of Commerce, *supra* note 84; 47 U.S.C. § 227 (c), 227 (f) (2000). *See*, Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection of 2001; Enforcement Decree of the Framework Act on Informationalization Promotion of 2002; Enforcement Decree of the Protection of Communication Secrets Act of 2002, *available at* http://www.moleg.go.kr (last visited Mar. 21, 2003).

[225] *See*, Beth Givens, *supra* note 74, at 352-4; Sun Kyung Kwun, *supra* note 178.

[226] *See, e.g.*, David J. Klein, *supra* note 45, at 394.

it would be relatively easier for the government to centrally regulate violations of consumer privacy, because it has a uniform legal system under a single court system.

The U.S. and Korea have in common that personal information is being protected by the sectoral regulations.[227] Such sectoral approach in protection of personal information purportedly has caused individuals' confusion and inefficiencies in protection of consumer privacy in the U.S. and Korea. In reality, however, preparation of easily understandable and common rules regulating consumer privacy is not an easy task.

The U.S. regulations on protection of personal information can be said to be distinctive from their Korean counterparts in that they are more commercially oriented, thus mostly being handled by the FTC. In Korea for the most part, protection of personal information is handled by the Ministry of Information and Communication,[228] which is an administrative department taking orders directly from the President whose goal is not only to protect individual interests but also to promote business activities. Accordingly, the Ministry of Information and Communication can be said to stand in a neutral position between the consumers and the businesses, while the FTC is more oriented toward protection of consumers.

Possibly Korea's protection of consumer information is being interpreted in the context of protection of individual rights of privacy rather than promotion of commercial activities.

---

[227] *See*, Beth Givens, *supra* note 74 at 348; Eun Woo Lee, *supra* note 167.

[228] *See*, Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection of 2001, *available at* http://www.moleg.go.kr (last visited Mar. 21, 2003).

In this regard, it may be suggested that Korea's regulatory practices are less sectoral and more centrally controlled than those of the U.S.

2. Legislation

In relation to the protection of consumer privacy, the FTC proposed fair information practices,[229] which would be most equivalent to the APICNUIP executed by the Ministry of Information and Communication of Korea[230], in that both of the regulations were codified to protect individuals from the violation of privacy by businesses and can be thought of as the most representative regulation for protection of online privacy.

However, the APICNUIP does not seem to provide standardized lists to be checked for protection of consumer privacy as fair information principles[231] do; rather, it stipulates such principles in an irregularly dispersed manner throughout the Act. For instance, the similar notion of notice/awareness, which is one of the five core principles suggested by the FTC[232], is found in Article 22 of the APICNUIP, while the same notion of integrity/security can be seen in Article 28 of the APICNUIP.[233]

Such unsystematic legislation in Korea may cause confusion and complexity to the consumers and the businesses as to what should be prioritized with concern for protection of consumer privacy. It may be suggested to the government of Korea that it needs to

---

[229] Federal Trade Commission, *supra* note 82, at 7-11.

[230] *See*, Act on Promotion of Information and Communications Network Utilization and Information Protection.

[231] *See*, Federal Trade Commission, *supra* note 82, at 7-11.

[232] *Id.*

[233] *See*, Act on Promotion of Information and Communications Network Utilization and Information Protection, art. 22 - 28.

simplify and itemize its regulatory targets, such as the five core principles of privacy protection proposed by the FTC.

The basic legislative frameworks of protection of personal information have been found to be the same in both the U.S. and Korea in that the entities subject to the legislation can be classified into two categories: the governmental agencies and private businesses. Included in the legislation regulating the governmental agencies are the FOIA and the Tax Reform Act of 1976 in the U.S. and the PODIA and the POPPIA in Korea.[234] On the other hand, the FCRA and the Right to Financial Privacy Act of the U.S., and the APICNUIP, the PCSA and UPCIA of Korea were legislated to regulate private businesses.[235]

3. Attitude of the Courts

The U.S. federal courts have been shown to stand firm against violation of consumer privacy[236] based on Exemption 6 of the FOIA,[237] while state courts do not seem to be prepared with clear and codified rules to protect consumer information from commercial exploitation without consent.[238] Similarly, the Korean courts have been found to be more

[234] *See*, 5 U.S.C. § 552 (2000); 26 U.S.C. § 6103 (1994); Public Organization's Disclosure of Information Act art.7; Public Organization's Protection of Personal Information Act, art. 1.

[235] *See*, 15 U.S.C. §§ 1681-1681t (1994); 12 U.S.C. §§ 3401-3422 (1994); Act on Promotion of Information and Communications Network Utilization and Information Protection, art. 1.; Protection of Communication Secrets Act of 2002, art. 1.; Use and Protection of Credit Information Act art. 1.

[236] *See, e.g.*, 737 F.2d at 787 (9th Cir. 1984); 523 F. Supp. 11 at 14 (S.D.N.Y. 1980).

[237] 5. U.S.C. § 552 (b) (6) (2000).

[238] *See*, David Klein, *supra* note 45, at 402; 652 N.E.2d at 1351 (Ill. App. Ct. 1995).

favorable to protection of personal information from governmental agencies than from private industries.[239]

In protecting personal information from governmental agencies, the Korean courts apply the PODIA[240] and the POPPIA[241] and the U.S. courts may apply the FOIA. One distinction of the Korean courts is that they are provided with the codified legislation of the APICNUIP[242] beforehand in case of businesses illegally use personal information. However state courts in the U.S. evaluate violation of privacy rights of personal information case-by-case with reference to the Restatement (Second) of Torts[243] and may differ in their interpretations of the Restatement, just as state common law differs from state-to-state both on liability and especially damages, so there is much less uniformity than would be obtained from a single court system applying a specific piece of legislation.

---

[239] *See*, Supreme Court of Korea, 96noo2439 (May 23, 1997); Appellate Court of Korea, 94Ku39262 (Aug. 24, 1995); Supreme Court of Korea, Sunko99do6 (July 28, 2000); Administrative Court of Korea, 98Ku3692 (Feb. 25, 1999).

[240] Public Organization's Disclosure of Information Act, art. 4, cl. 1.

[241] Public Organization's Protection of Personal Information Act, art. 1.

[242] Act on Promotion of Information and Communications Network Utilization and Information Protection, art. 1.

[243] Restatement (Second) of Torts 652 (1977).

CHAPTER 4

DISPUTE RESOLUTION

With e-commerce being globalized, protection of consumer privacy has been a regulatory target in international as well as domestic transactions. An action brought against violation of consumer privacy in the international commerce between the U.S. and Korea is expected to encounter international legal barriers, which may not be of concern to domestic litigation but certainly is to international litigation. This chapter explores international legal issues that are likely to arise in the process of dispute resolution with respect to consumer privacy in electronic commerce between the U.S. and Korea to identify legal barriers between the two countries, and to provide an efficient mechanism to overcome such barriers.

A. Regulatory Systems

The regulatory systems to protect personal information were compared between the U.S. and Korea in Chapter 3 based on three criteria including the regulatory authorities, legislation and attitudes of the court. This section will investigate the ways the differences derived from the comparisons made in Chapter 3 will influence dispute resolution between the U.S. and Korea.

1. Conflicts of Regulatory Authorities

There exists a significant difference in the regulatory authorities between the U.S. and Korea in that the U.S. has two different layers (i.e., federal and state levels) of authorities to regulate the privacy of personal information, while Korea has only one system consisting of the regulatory authorities based on the administrative power including the Minister of Information and Communication, the Ministry of Government Administration and Home Affairs and the Ministry of Finance and Economy.[244]

Such differences in the systems of regulatory authorities is not likely to cause any serious confusion to U.S. businesses, because U.S. companies need to only be concerned with the administrative authorities empowered by the central government of Korea, while the Korean businesses should be concerned with the legal complexities of facing both the U.S. federal and state regulatory authorities. The difficulty caused by the difference in regulatory authority systems may be removed when a bilateral agreement is concluded recognizing the obligations of both countries to observe common rules to protect consumer privacy (such as the safe harbor principles).[245] The standardization of rules between the two countries would help Korean businesses to obviate their ignorant violation of consumer privacy rights in the U.S.

---

[244] *See*, Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection; Enforcement Decree of the Framework Act on Informationalization Promotion; Enforcement Decree of the Protection of Communication Secrets Act; Enforcement Decree of the Public Organization's Protection of Personal Information Act; Enforcement Decree of the Public Organization's Disclosure of Information Act; Enforcement Decree of the Use and Protection of Credit Information Act.

[245] *See*, U.S. CONST. art. VI ("...; and all Treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land..."; also see KOREA CONST. art. 6 cl.1, "Both treaties concluded by the Constitution and international customary laws shall have the same validity as the municipal laws.").

In addition, the FTC was found to be different from the Ministry of Information and Communication in that the FTC targets its regulatory goal to protection of consumer privacy, while the Ministry of Information and Communication has mainly regulated violation of information privacy in general rather than in the context of consumer protection.[246]

Individual consumer rights may well have to be separated from general civil rights with respect to their legal protection, because the positions of individual consumers are inferior to businesses in terms of negotiation powers and financial status; thus it may be highly probable that they cannot protect their own rights as a consumer without special treatment by the regulatory authorities as the FTC provides in the U.S.

Therefore, it would be necessary that the current regulatory function of consumer privacy should be transferred from the Ministry of Information and Communication to the Korea Consumer Protection Agency established by the Consumer Protection Act,[247] which will not only foster its specialty to protect consumer privacy and but also accomplish compatibility between the regulatory authorities of the U.S. and Korea.[248]

2. Conflicts of Legislation

With the preparation of fair information practices, the FTC has maintained fairly clear and standardized rules to be kept by businesses to protect consumer privacy.[249] However, the

---

[246] *See*, Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection.

[247] Consumer Protection Act (last revised Mar. 28, 2001), ch. 4, *available at* http://www.moleg.go.kr (last visited Mar. 21, 2003).

[248] It may need to be expressly stipulated in the Consumer Protection Act that Korea Consumer Protection Agency shall be in charge of protection of online consumer privacy.

[249] Federal Trade Commission, *supra* note 82, at 7-11.

APICNUIP has not provided the same type of clear and itemized rules; but rather has dispersed the rules protecting personal information throughout the Act in an ambiguous manner.[250] Thus, it would be advisable that the APICNUIP should be revised to spotlight important points (e.g., Notice/Awareness, Choice/Consent, etc.) more clearly.

In addition, the APICNUIP was passes to protect information privacy in general rather than consumer privacy in particular; thus, it would be necessary to promulgate a directive specially designed for protection of consumer privacy in order for the Korean legislation to be compatible with U.S. fair information practices.

3. Conflicts in the Attitudes of the Courts

The attitude of the U.S. courts toward protection of consumer privacy do not seem to be much different from those of Korean courts.[251] However, the state courts in the U.S. have relied on the law of torts to protect individual information privacy from illegal use by businesses, while the Korean courts are equipped with the codified rules (e.g. the APICNUIP).[252] Accordingly, the U.S. courts may need more legal rulings in favor of consumers providing the legal justification for protecting consumer privacy than do the Korean courts, which would make it more difficult for individuals to protect their privacy in the state courts of the U.S. Therefore, it seems reasonable that a codified rule to protect

---

[250] *See*, *id*.

[251] *See*, Supreme Court of Korea, 96noo2439 (May 23, 1997); Appellate Court of Korea, 94Ku39262 (Aug. 24, 1995); Supreme Court of Korea, Sunko99do6 (July 28, 2000); Administrative Court of Korea, 98Ku3692 (Feb. 25, 1999).

[252] *See*, Act on Promotion of Information and Communications Network Utilization and Information Protection, art. 1.; Restatement (Second) of Torts 652 (1977).

consumer privacy from businesses needs to be legislated to provide the same level of readiness in finding legal justification in lawsuits in the U.S. and Korea.

B. International Jurisdiction

Among the three kinds of jurisdiction,[253] only judicial jurisdiction[254] will be examined for disputes over consumer privacy in international e-commerce. Legislative jurisdiction[255] deals with choice of substantive laws which were already substantially investigated in Chapter 3, and several suggestions were made to cure the discrepancies in legislation found between the two countries in section A of Chapter 4. In addition, violation of consumer privacy stems from tort law; thus the laws of the forum state would be applied in most cases. Enforcement jurisdiction[256] does not seem to be as significant as an Internet-specific legal issues as much as the other two types of jurisdiction, because enforcement is physically executed by the law enforcement of the forum state without involvement of the Internet.

---

[253] LORI F. DAMROSCH ET. AL., INTERNATIONAL LAW, 1088 (4th ed. 2001) ("Traditionally three kinds of jurisdiction are distinguished: legislative, judicial, and executive or enforcement jurisdiction.").

[254] According to Restatement (Third) of Foreign Relation Law 401 (b), judicial jurisdiction is defined as the authority of a State "subject persons or things to the process of its courts or administrative tribunals, whether in civil or in criminal proceedings, whether or not the state is a party to the proceedings."

[255] According to According to Restatement (Third) of Foreign Relation Law 401 (a), legislative jurisdiction is defined as the authority of a State "to make its law applicable to the activities, relations, or status of persons, or the interests of persons in things, whether by legislation, by executive act or order, by administrative rule or regulation, or by determination of a court."

[256] According to According to Restatement (Third) of Foreign Relation Law 401 (c), enforcement jurisdiction refers to "inducing or compelling compliance or to punishing noncompliance with its laws or regulations, whether through the courts or by use of executive, administrative, police, or other nonjudicial action."

1. Disputes over Consumer Privacy in E-Commerce

Violation of e-consumer privacy is not only regulated by civil law (e.g., redress)[257] but also by criminal law (e.g. a hacker's attack on databases of the Internet server).[258] Most of the legal actions in regard to violation of consumer privacy would be related with management of consumer information, including collection, maintenance/dissemination, and discard.[259] Illegal actions related to consumer data may be committed when businesses collect a consumer's personal information without consent. In addition, Internet hackers may have illegal access to customer databases when businesses negligently maintain or discard the data files.

In general, legal issues related with judicial jurisdiction in international e-commerce will become more complicated considering the legal characters of cyberspace in which an action is physically performed.[260] For instance, among the three types of violation of online consumer privacy, illegal actions involved with collection of consumer information may become more complicated in determining judicial jurisdiction when each party claims its own forum based on arguments that the illegal action (e.g., collection of consumer information without consent) is committed in that party's own forum through the Internet. On the other hand, the other two activities, maintenance/dissemination and discard of

[257] *See*, Federal Trade Commission, *supra* note 107.

[258] Tapio Puurunen, *The Legislative Jurisdiction of States Over Transactions in International Electronic Commerce*, 18 J. MARSHALL J. COMPUTER & INFO. L. 689, 699 (2000).

[259] Consumer information can be managed with the multiple of stages including collection, maintenance, and discard. In the collection stage, consumer information may be initially gathered and stored into a database. During the maintenance stage, consumers' personal information may be updated and changed. For the stage of discard, consumers' personal data may be deleted when they are outdated and useless.

[260] The territoriality principle of international jurisdiction may be completely obsolete in the era of cyberspace, because the Internet space is not physically identifiable.

consumer information, are conducted without interaction between consumers and businesses through the Internet; thus, violation of consumer privacy related to these two activities are not likely to be subject to the legal intricacies arising from Internet jurisdiction but are under the traditional legal realm of international jurisdiction.

Faced with the advent of e-commerce, three basic theories have emerged to resolve controversies over personal jurisdiction in international e-commerce:[261] the territoriality principle,[262] the effects doctrine,[263] and the sufficient minimum contacts approach.[264] However, the territoriality principle does not seem to be applicable to the legal issues of judicial jurisdiction in cyberspace because cyberspace does not have a tangible territory.[265] Thus, the effects doctrine and the sufficient minimum contacts approach have been mostly applied in deciding cyberspace jurisdiction in international e-commerce.[266]

2. Judicial Jurisdiction over E-Consumer Privacy in the U.S. and Korea

In relation to the issue of jurisdiction over extraterritorial persons, the U.S. courts have embraced the sufficient minimum contacts test with the emphasis on the actual conduct of

---

[261] GERALD R. FERRERA, ET. AL., CYBERLAW: TEXT AND CASE 14-33 (2000); Lucille M. Ponte, *Boosting Consumer Confidence in E-Business: Recommendations for Establishing Fair and Effective Dispute Resolution Programs for B2C Online Transactions*, 12 ALB. L. J. SCI & TECH. 441, 482-3 (2002).

[262] Tapio Puurunen, *supra* note 258, at 703-6 (The territoriality principle denotes that a nation or state would exert judicial power over persons within its territory).

[263] Lucille M. Ponte, *supra* note 261, at 483 ("The effects approach puts an emphasis on the damaging impact of the extraterritorial party's conduct within a foreign forum as a basis for exercising jurisdiction.").

[264] *Id.* (The sufficient minimum contacts approach tests "whether: a) the defendant has purposefully made continuos and systematic contacts with the forum, b) the litigation arises out of these contacts, and c) the exercise of extraterritorial jurisdiction is reasonable and fair.").

[265] *See*, Aristotle G. Mirzaian, *Y2K Who Cares? We have Bigger Problems: Choice of Law in Electronic Contracts*, 6 RICH. J. L. & TECH. 20, 85-7 (1999).

[266] Lucille M. Ponte, *supra* note at 261, 483.

e-businesses.[267] For instance, in *Burger King Corp. v. Rudzewicz*, the U.S. Supreme Court stated that minimum contacts should be a constitutional basis for jurisdiction in the forum state,[268] quoting from *World-Wide Volkswagen Corp* . v. *Woodson* that the foreseeability of causing *injury* in another State is not a "sufficient benchmark"[269] to establish minimum contacts; rather foreseeability should be interpreted such that "the defendant should reasonably anticipate being haled into court there."[270]

The U.S. courts seem to have put more emphasis on tightening the compliance requirements of the minimum contacts for e-business so as to allow it to thrive as an engine for the domestic economy.[271] Such trend may be found in the U.S. district court's decision,[272] where the purposeful availment standard that the defendant should have "an intent or purpose to serve the market in the forum State"[273] was suggested to establish minimum contacts, replacing the foreseeability requirement specified in *World-Wide Volkswagen Corp* . v. *Woodson*.[274]

In relation to personal jurisdiction over the Internet business, the U.S. court ruled in *Zippo Mfg. Inc. v. Zippo Dot Com, Inc.* that the nonresident defendant should be subject to the plaintiff's forum, based on "examining the level of interactivity and commercial nature of the exchange of information that occurs on the Web site."[275] The court further stated that a

---

[267] GERALD R. FERRERA, ET. AL., *supra* note 261, at 345.
[268] 471 U.S. 462, 474 (1985).
[269] 444 U.S. 289, 295. (1980).
[270] 444 U.S. at 297 (1980).
[271] *See*, Lucille M. Ponte, *supra* note 261, at 484.
[272] *In re* DES Cases, 789 F. Supp. 552, 584 (1992).
[273] Asahi Metal Industry Co. v. Superior Court of California, 480 U.S. 102, 112 (1987).
[274] 444 U.S. at 295. (1980).
[275] 952 F. Supp. 1119, 1124 (1997).

passive Web site that is open to public for the sole purpose of information can not be the grounds for exercise of personal jurisdiction.[276] More specifically, in *Euromarket Designs, Inc. v. Crate & Barrel Ltd.*, the court derived a robust condition for a web-based business activity to be subject to the forum state that the e-business should be engaged in transactions "purposefully and consistently".[277]

Violation of consumer privacy has been subject to the personal jurisdiction principle of "substantial interactivity" in the forum state in *Myers v. Bennett Law Offices*, where the court ruled that personal jurisdiction should be given because the defendant "purposefully" exposed itself to the State of Nevada by "intentionally" organizing its activities in that state; also a substantial part of the actions that caused the claim occurred in Nevada.[278] Accordingly, it is highly probable that the U.S. courts will support the principle of substantial interactivity in decisions regarding personal jurisdiction with respect to online consumer privacy.

In Korea, the law of civil procedure provides that judicial jurisdiction with respect to torts should be exercised where the tortious action occurred;[279] thus violation of consumer privacy may be adjudicated in the jurisdiction where such violation is proved to have happened.[280] In lawsuits brought against violation of consumer privacy in electronic commerce, the litigation is most likely to be filed in the plaintiff's jurisdiction to make the judicial process more affordable and favorable. The International Civil Law of Korea states that the courts

---

[276] 952 F. Supp. at 1124 (1997).
[277] 96 F. Supp. 2d 824, 828 (N.D. Ill. 2000).
[278] 238 F.3d 1068, 1068 (2001).
[279] KOREA CIVIL PROCEDURE CODE, art. 16 cl.1.
[280] Supreme Court of Korea, 73ma815 (1973).

shall exercise judicial jurisdiction over international disputes based on evaluation of the substantial connectivity of the dispute with Korea.[281]

It may be suggested that the U.S. fundamental principles of international jurisdiction are similar to Korea's in that both countries activate 'substantial interactivity' with the forum state to determine personal jurisdiction.

C. International Arbitration

To resolve international disputes, several alternatives for dispute resolution have been offered, including arbitration, mediation, conciliation etc. Among all of the dispute resolution methods, international arbitration has been considered as having the most practical relevance in commercially oriented dispute resolution (i.e. international e-commerce).[282]

1. Characteristics

As an alternative to litigation, international arbitration has been widely recommended for resolving disputes over violation of consumer privacy in international e-commerce due to its unique advantages.[283] The standardized procedure of dispute resolution throughout the world would be an additional advantage of international arbitration, making a significant

---

[281] International Civil Act, art. 2, cl.1 (last revised in 2001), *available at* http://www. moleg.go.kr, (last visited Mar. 20, 2003).

[282] CHRISTIAN BÜHRING-UHLE, ARBITRATION AND MEDIATION IN INTERNATIONAL BUSINESS 261 (1996).

[283] CHRISTIAN BÜHRING-UHLE, *supra* note 282, at 87 (International arbitration has been reported to be advantageous to dispute resolution in that: it ensures a competent tribunal, flexibility of the procedure, a reasonably predictable and legitimate decision by a tribunal, achieves final and enforceable awards, and excludes competing procedures practically on a worldwide scale).

contribution to overcoming the legislative and judicial differences between the U.S. and Korea.

One of the important attributes of international arbitration is the agreement[284] between the two parties to be bound by the arbitration award.[285] Most international arbitrations are conducted pursuant to a contractual arbitration clause included in the principal (underlying) contract,[286] which attempts to provide a procedure for resolving future conflict between the parties.

Considering the difficulties of international litigation due to the legal differences found between the U.S. and Korea, disputes over online consumer privacy had best be resolved by international arbitration. Among the two types of arbitration agreements, the pre-contractual agreement of arbitration is likely to be more efficient than the post-contractual agreement, because in the pre-contractual agreement, the dispute resolution process is stipulated in advance; thus it will save on the total time and costs of arbitration process. Otherwise a significant amount of time and costs may be wasted just negotiating the agreement to arbitrate.

2. Arbitration Institutions

The arbitration institutions available for resolution of disputes over violation of online consumer privacy should be able to deal with private disputes, because at least one of the

---

[284] *Id.*, at 43 (There are two types of arbitration agreements, "the submission of future disputes through an arbitration clause that is included in or annexed to the principal contract, or the submission of an existing dispute to arbitration by means of a submission agreement").

[285] *Id.*

[286] ALAN REDFERN & MARTIN HUNTER, LAW AND PRACTICE OF INTERNATIONAL COMMERCIAL ARBITRATION 53 (2d ed. 1991).

parties involved with the dispute is an individual consumer. Although claims regarding online consumer privacy are not a primary substance of contract in e-commerce and are based on tort, they are raised in the context of commerce between the consumer and the business. Therefore, it would be natural that such claims should be resolved by commercial arbitration institutions.

The commercial arbitration institutions potentially available for disputes over online consumer privacy include the International Court of Arbitration of the International Chamber of Commerce (hereinafter "ICAICC")[287], the Commercial Arbitration and Mediation Center for the Americas of American Arbitration Association (hereinafter "CAMCA"),[288] and the Korean Commercial Arbitration Board (hereinafter "KCAB").[289] Each of these arbitration institutions provides its own standard arbitration clauses[290] in order to obviate confusions resulting from ambiguous wording in arbitration agreements. The procedure and the

---

[287] *See*, International Chamber Commerce, Rules of Arbitration (in force as from 1 January 1998), art. 1, cl.1., *available at* http://www.iccwbo.org/ court/ english/ arbitration/ rules.asp (last visited May, 20, 2003).

[288] *See*, Commercial Arbitration and Mediation Center for the Americas, Arbitration Rules, art. 1, cl.1., *available at* http://www.adr.org (last visited May 20, 2003).

[289] *See*, Korea Arbitration Act (last revised 2002), Supplementary Provision #3.

[290] The standard ICC arbitration clause: "All disputes arising out of or in connection with the present contract shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce by one or more arbitrators appointed in accordance with the said Rules.", *available at* http://www.iccwbo.org/ court/ english/ arbitration/ model_clause.asp (last visited May 20, 2003). The CAMCA standard arbitration clause: "Any dispute, controversy or claim arising out of or relating to this contract, or the breach thereof, shall be finally settled by arbitration administered by the Commercial Arbitration and Mediation Center for the Americas in accordance with its rules and judgment on the award rendered by the arbitrator(s) may be entered in any court having jurisdiction thereof.", *available at* http://www.adr.org (last visited May 20, 2003). The KCAB standard arbitration clause: “All disputes, controversies, or differences which may arise between the parties, out of or in relation to or in connection with this contract, or for the breach thereof, shall be finally settled by arbitration in Seoul, Korea in accordance with the Arbitration Rules of the Korean Commercial Arbitration Board and under the Laws of Korea. The award rendered by the arbitrator(s) shall be final and binding upon both parties concerned.", *available at* http://www.kcab.or.kr/ M2/ M2_S6.asp (last visited May 20, 2003).

governing law of the arbitration are prescribed in each of the standard arbitration clauses by inserting it into the principal contract.

The claims that may be brought to protect online consumer privacy and redress damages thereof have a legal basis in torts, in which case the forum state usually applies its own laws. If the parties attempt to resolve the dispute through litigation, the resolution process may be deadlocked by controversies triggered by choice of law and international jurisdiction issues, etc. Accordingly, international arbitration had better be put as a priority when selecting a method to resolve international disputes over online consumer privacy.

CHAPTER 5

SUGGESTIONS AND FUTURE RESEARCH

Both protections of consumers' online privacy and promotion of e-commerce have been major regulatory targets for most of the countries since the inception of online business. Legal alternatives have been sought to cope with the conflicting interests between consumers and e-businesses in the context of international e-commerce. Several incompatible characteristics of regulating consumer privacy in e-commerce between the U.S. and Korea are summarized in this chapter. In addition, curative suggestions are made to establish a new legal framework to protect online consumer privacy without contraction of e-business between the U.S. and Korea.

First, Korea's regulations for protecting online consumer privacy were found to be centrally controlled, while the U.S. authorities have encouraged self-regulation. Considering the long run efficiency of self-regulation, the Korean authorities should seek more self-regulatory measures and establish consensus among the businesses to voluntarily protect consumer online privacy.

Second, due to the difference in the court systems between the U.S. and Korea, it is difficult to take standardized regulatory measures throughout the U.S., while it is relatively easier for the Korean government to regulate violations of online consumer privacy with standardized measures, because its legal system is uniform under one court system. Another

distinction between Korean and U.S. courts is that the Korean courts decide cases on the basis of codified rules, while the U.S. state courts evaluate violation of consumer privacy on a case-by-case basis.

Third, it has been revealed that U.S. regulations on protection of online consumer privacy are for the most part commercially oriented and controlled by the FTC, whereas in Korea, an administrative department, the Ministry of Information and Communication, regulates online consumer privacy as a primary authority, resulting in lack of specialization in the matters of consumer protection. To improve the efficiency and specialization in regulation of online consumer privacy in Korea, it would be necessary to promulgate a directive specially designed for protecting consumer privacy and delegating the regulatory power to the Korea Consumer Protection Agency established by the Consumer Protection Act.[291] Such delegation would accomplish a balance of the regulatory authorities between the U.S. and Korea in that both authorities would be founded upon consumer protection.

Fourth, Korea's APICNUIP has been revealed to be less clear than the FTC's five core principles of fair information practices in that it is neither systematically organized nor orderly classified to make businesses and consumers readily informed of the specifics of the APICNUIP. It is recommended that the APICNUIP be revised to make the rules more organized and compatible with the FTC's fair information practices.

Finally, international arbitration is recommended as the best tool to resolve and prevent the intricacies of international litigation brought against violation of online consumer privacy. The arbitration institutions to deal with disputes over consumer privacy in e-

[291] Consumer Protection Act, ch. 4. (last revised Mar 28, 2001).

commerce between the U.S. and Korea may include the International Court of Arbitration of the International Chamber of Commerce, the Commercial Arbitration and Mediation Center for the Americas of American Arbitration Association, and the Korean Commercial Arbitration Board.

In addition to providing several suggestions and insights based on the comparative analysis of online consumer privacy between the U.S. and Korea, this study would have been better shaped if the following two aspects had been remedied and reflected in the analysis. First, due to lack of relevant cases in Korea, it was impossible to derive the attitudes of the Korean courts directly from commercial cases. Rather they were extrapolated metaphorically from the noncommercial cases.[292] Thus, it may be questionable how accurately their attitudes would be reflected in the commercial context of consumer protection. On the other hand, the attitudes of U.S., the courts toward online consumer privacy have been revealed in commercial cases, which eliminates this particular concern.[293] Therefore, this study needs to be updated to include the attitudes of Korean courts as commercial cases become available.

Second, the proposed dispute resolution method of international arbitration was designed only with reference to a set of two countries (the U.S. and Korea). Therefore, it may not be representative of the international e-commerce disputes. Considering the fact that online consumer privacy should be protected not only between these two countries but also in a

---

[292] *See*, *e.g.*, Supreme Court of Korea, 96noo2439, (May 23, 1997); Appellate Court of Korea (Seoul), 94Ku39262, (Aug 24, 1995); Supreme Court of Korea, Sunko99do6 (July 28, 2000); Administrative Court of Korea (Seoul), 98Ku3692 (Feb. 25, 1999).

[293] *See e.g.*, 737 F.2d at 787 (9th Cir. 1984); 523 F. Supp. 11 at 14 (S.D.N.Y. 1980); 502 F.2d at 137 (3rd Cir. 1974).

global context, an internationally recognized dispute resolution system may have to be further developed in future research to promote online consumer privacy worldwide.

REFERENCES

<U.S. Sources>

Legislation

1. 5 U.S.C. § 552 (1994).
2. 5 U.S.C. § 552 (2000).
3. 12 U.S.C. § 3401-3422 (1994).
4. 15 U.S.C. §§ 41-58 (2001).
5. 15 U.S.C. § 45 (a) (1994).
6. 15 U.S.C. § 1125(d) (2001).
7. 15 U.S.C. §§ 1681-1688t (1994).
8. 15 U.S.C. §§ 6501-6506 (2001).
9. 17 U.S.C. §§ 1201-1205 (2001).
10. 18 U.S.C. §§ 2510-2511 (1994).
11. 18 U.S.C. §§ 2710-2711 (1994).
12. 20 U.S.C. § 1232g (1994).
13. 26 U.S.C. § 6103 (1994).
14. 42 U.S.C. § 2000aa (2000).
15. 47 U.S.C. § 227 (2000).

16. 47 U.S.C. § 551 (a) (1994).

17. U.S. CONSTITUTION.

Cases

1. Asahi Metal Industry Co. v. Superior Court of California, 480 U.S. 102 (1987).

2. Burger King Corp. v. Rudzewicz, 471 U.S. 462 (1985).

3. Dwyer v. American Express Co., 652 N.E.2d 1351 (Ill. App. Ct. 1995).

4. Euromarket Designs, Inc. v. Crate & Barrel Ltd., 96 F. Supp. 2d 824 (N.D. Ill. 2000).

5. HMG Marketing Association v. Freeman, 523 F. Supp. 11 (S.D.N.Y. 1980).

6. *In re* DES Cases, 789 F. Supp. 552 (1992).

7. *In re* GeoCities, Inc., No. C-3849, 1999 FTC LEXIS 17 (FTC Feb. 5, 1999).

8. Minnis v. United States Dep't of Agriculture, 737 F.2d 784 (9th Cir. 1984).

9. Moran Towing & Transp. Co. v. United States, 56 F. Supp. 105 (E.D.N.Y. 1991).

10. Myers v. Bennett Law Offices, 238 F.3d 1068 (2001).

11. Scottsdale Unified Sch. Dist. No. 48 v. KPNX Broad. Co, 191 Ariz. 297 (1998).

12. United States Dep't of Justice v. Reporters Committee for Freedom, 489 U.S. 749 (1989).

13. Wine Hobby USA, Inc. v. United States IRS, 502 F.2d 133 (3rd Cir. 1974).

14. World-Wide Volkswagen Corp . v. Woodson, 444 U.S. 289 (1980).

15. Zippo Mfg. Inc. v. Zippo Dot Com, Inc., 952 F. Supp. 1119 (1997).

Secondary sources

1. A. BRECKENRIDGE, THE RIGHT TO PRIVACY (1970).

2. A. WESTIN, PRIVACY AND FREEDOM 7 (1967).

3. ALAN REDFERN & MARTIN HUNTER, LAW AND PRACTICE OF INTERNATIONAL COMMERCIAL ARBITRATION (2d ed. 1991).

4. Aristotle G. Mirzaian, *Y2K Who Cares? We have Bigger Problems: Choice of Law in Electronic Contracts*, 6 RICH. J. L. & TECH. 20 (1999).

5. Beth Givens, *Symposium on Internet Privacy: Privacy Expectations in a High Tech World*, 16 SANTA CLARA COMPUTER & HIGH TECH. L. J. 347 (2000).

6. *Business Week/Harris Poll: Online Insecurity*, Business Week, March 16, 1998.

7. CHRISTIAN BÜHRING-UHLE, ARBITRATION AND MEDIATION IN INTERNATIONAL BUSINESS (1996).

8. Commercial Arbitration and Mediation Center for the Americas, Arbitration Rules, *available at* http://www.adr.org (last visited May 20, 2003).

9. Debra A. Valentine, *Symposium on Internet Privacy: Privacy on the Internet: The Evolving Legal Landscape*, 16 COMPUTER & HIGH TECH. L. J. 401 (May 2000).

10. Dorothy Glancy, *Symposium At The Intersection of Visible and Invisible Worlds: United States Privacy and The Internet*, 16 SANTA CLARA COMPUTER & HIGH TECH. L. J.357 (2000).

11. Elinor Mills Abreu, *FBI probing theft of 8 million credit card numbers*, AOL BUSINESS NEWS, Feb. 19, 2003, *at* http://my.aol.com (last visited Mar. 6, 2003).

12. Federal Trade Commission (FTC), Privacy Online: A Report To Congress (1998), *at* http://www.ftc.gov/ reports/ privacy3/ toc.htm (last visited Mar. 9, 2003).

13. Federal Trade Commission, Privacy Online: Fair Information Practices in the Electronic Marketplace (May 2000), *at* http:// www.ftc.gov/ reports/ privacy2000/ privacy 2000text.pdf (last visited Mar. 10, 2003).

14. Federal Trade Commission Report, Self-Regulation and Privacy Online, *at* http://www.ftc.gov/os/ 1999/ 9907/ pt071399.htm (last visited Mar. 11, 2003).

15. Fred H. Cate, *Principles of Internet Privacy*, 32 CONN. L. REV. 877 (2000).

16. GARTH SALONER & A. MICHAEL SPENCE, CREATING AND CAPTURING VALUE (2002).

17. GARY P. SHNEIDER & JAMES T. PERRY, ELECTRONIC COMMERCE (2001).

18. GERALD R. FERRERA, ET. AL., CYBERLAW: TEXT AND CASE (2000).

19. GERALD SPINDLER & FRITJOF BÖRNER, E-COMMERCE LAW IN EUROPE AND THE USA, (2002).

20. James P. Nehf, *Recognizing The Societal Value in Information Privacy*, 78 WASH. L. REV. 1 (2003).

21. Joe Queenan, *My Mail Insecurity; What If the Neighbors See What the Junk Marketers Send Me?*, The Wash. Post, Oct. 22, 1995.

22. Jordan M. Blanke, *"Safe Harbor" and the European Union's Directive on Data Protection*, 11 ALB. L. J. SCI. & TECH. 57 (2000).

23. LEON G. SCHIFFMAN & LESLIE LAZAR KANUK, CONSUMER BEHAVIOR (7th ed. 2000).

24. LORI F. DAMROSCH ET. AL., INTERNATIONAL LAW (4th ed. 2001).

25. Lucille M. Ponte, *Boosting Consumer Confidence in E-Business: Recommendations for Establishing Fair and Effective Dispute Resolution Programs for B2C Online Transactions*, 12 ALB. L. J. SCI & TECH. 441 (2002).

26. Michael Cordera, *NOTE AND COMMENT: E-Consumer Protection: A Comparative Analysis of EU and US Consumer Protection on the Internet*, 27 RUTGERS COMPUTER & TECH. L. J. 231 (2001).

27. MICHAEL R. SOLOMON & ELNORA W. STUART, MARKETING (2nd ed. 2000).

28. Mozelle W. Thompson, *Presentation: The Challenges of Law in Cyberspace-Fostering the Growth an Safety of E-Commerce*, 6 B. U. SCI. & TECH. L. 1 (2000).

29. Omar Saleem, *The Establishment of A U.S. Federal Data Protection Agency to Define and Regulate Internet Privacy and Its Impact on U.S. -China Relations: Marco Polo Where Are You?*, 19 J. MARSHALL J. COMPUTER & INFO. L. 172 (2000).

30. Pamela Samuelson, *Five Challenges for Regulating the Global Information Society*, *in* REGULATING THE GLOBAL INFORMATION SOCIETY 311 (Christopher T. Marsden ed., 2000).

31. PAUL SHAW, E-BUSINESS PRIVACY AND TRUST (2001).

32. RAFI A. MOHAMMED, ROBERT J. FISHER, BERNARD J. JAWORSKI & AILEEN M. CAHILL, INTERNET MARKETING (2002).

33. Restatement (Second) of Torts 652 (1977).

34. Restatement (Third) of Foreign Relation Law 401.

35. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890).

36. Tapio Puurunen, *The Legislative Jurisdiction of States over Transactions in International Electronic Commerce*, 18 J. MARSHALL J. COMPUTER & INFO. L. 689 (2000).

37. U.S. Department of Commerce, Introductory Welcome Statement, *at* http://www. export. gov/ safeharbor (last visited Mar. 15, 2003).

38. U.S. Department of Commerce, Safe Harbor Overview, *at* http://www.export.gov/ safeharbor/sh_overview.html (last visited Mar. 9, 2003).

39. U.S. Department of Commerce, Safe Harbor Privacy Principles (2000), *at* http:// www. export.gov/safeharbor/SHPRINCIPLESFINAL.htm (last visited Mar. 9, 2003).

40. WASHIM E. RAJPUT, E-COMMERCE SYSTEMS ARCHITECTURE AND APPLICATIONS (2000).

41. William S. Challis & Ann Cavoukian, *The Case for A U.S. Privacy Commissioner: A Canadian Commissioner's Perspective*, 19 J. MARSHALL J. COMPUTER & INFO. L. 1 (2000).

<Korean and International Sources>

Legislation

1. Act on Promotion of Information and Communications Network Utilization and Information Protection of 2002, *available at* http://www.moleg. go.kr (last visited Mar. 21, 2003).

2. Consumer Protection Act (last revised Mar. 28, 2001), ch. 4, *available at* http://www.moleg.go.kr (last visited Mar. 21, 2003).

3. Council Directive 95/96, 1995 O.J. (L 281) 31.

4. Electric Communications Business Act, *available at* http://www. moleg.go.kr, (last visited Mar. 22, 2002).

5. Enforcement Decree of the Framework Act on Informationalization Promotion of 2002, *available at* http://www.moleg.go.kr (last visited Mar. 21, 2003).

6. Enforcement Decree of the Act on Promotion of Information and Communications Network Utilization and Information Protection of 2001, *available at* http:// www.moleg.go.kr (last visited Mar. 21, 2003).

7. Enforcement Decree of the Protection of Communication Secrets Act of 2002, *available at* http://www.moleg.go.kr (last visited Mar. 21, 2003).

8. Enforcement Decree of the Public Organization's Disclosure of Information Act of 1996 (last revised in 1999), *available at* http://www.moleg.go.kr (last visited Mar. 21, 2003).

9. Enforcement Decree of the Public Organization's Protection of Personal Information Act of 1995, *available at* http://www.moleg.go.kr (last visited Mar. 21, 2003).

10. Enforcement Decree of the Use and Protection of Credit Information Act of 1995, *available at* http://www.moleg.go.kr (last visited Mar. 21, 2003).

11. EUR-Lex: Community Legislation in Force, Directive 95/46/EC of the European Parliament and the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 995 O.J. (L281) 31 (November 23, 1995), *available at* http://www.lexis.com (last visited Mar. 15, 2003).

12. Framework Act on Informationalization Promotion of 2002; Protection of Communication Secrets Act of 2002, *available at* http://www.moleg.go.kr (last visited Mar. 21, 2003).

13. International Chamber Commerce, Rules of Arbitration (in force as from 1 January 1998), *available at* http:// www.iccwbo.org/court/english/arbitration/rules.asp (last visited May 20, 2003).

14. International Civil Act, (last revised in 2001), *available at* http://www. moleg.go.kr, (last visited Mar. 20, 2003).

15. Korea Arbitration Act (last revised 2002).

16. KOREA CIVIL CODE.

17. KOREA CIVIL PROCEDURE CODE.

18. KOREA CONSTITUTION.

19. Promotion of Information Networks and Protection of Personal Information Act of 2000, *available at* http://www. moleg. go.kr (last visited Mar 21, 2003).

20. Protection of Communication Secrets Act of 2002, *available at* http:// www.moleg.go.kr (last visited Mar. 21, 2003).

21. Public Organization's Disclosure of Information Act of 1996, *available at* http://www.moleg.go.kr (last visited Mar 21, 2003).

22. Public Organization's Protection of Personal Information Act of 1994, *available at* http://www. moleg. go.kr (last visited Mar 21, 2003).

23. Use and Protection of Credit Information Act of 2002, *available at* http://www. moleg.go.kr, (last visited Mar. 20, 2003).

Cases

1. Administrative Court of Korea, 98Ku3692 (Feb. 25, 1999).
2. Appellate Court of Korea, 94Ku39262 (Aug. 24, 1995).
3. Korea Constitutional Court, 88 Hunma 22 (Sep. 4, 1989).
4. Korea Constitutional Court, 90 Hunma 133 (May 13, 1991).
5. Korea Constitutional Court, 92 Hunba 31 (Dec. 29, 1994).
6. Korea Constitutional Court, 93 Hunma 174 (Aug. 31, 1994).
7. Supreme Court of Korea, 73ma815 (1973).
8. Supreme Court of Korea, 96noo2439 (May 23, 1997).
9. Supreme Court of Korea, Sunko99do6 (July 28, 2000).

Secondary sources

1. CHEOL SOO KIM, THE CONSTITUTION OF KOREA (2000).
2. EU Council of Europe, Recommendation No R (99) 5 of the Committee of Ministries to Member states for the Protection of Privacy on the Internet (1999), *at* http://www.coe. fr/cm/ta/rec/1999/99r5.htm (last visited Mar. 9, 2003).
3. Eun Woo Lee, *Legal Issues on Privacy and Protection of Personal Information*, Symposium Reports of Civil Activists Associates for Protection of Privacy 1 (2001), *at* http://www. privacy.or.ke/ privacy.text.htm (last visited Mar. 21, 2003).

4. Jung Hee Lee, *A Desperate Measure to Cope with Illegal Dissemination of Bank Passwords,* The Pusanilbo, Jan. 22, 2003.

5. Korea Information Security Agency, Reports on Information Security Efforts by Selected Private Sectors: As for Year 2001 (2002).

6. Organization for Economic Cooperation and Development (OECD), Recommendation of the Council Concerning Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980), *at* http://europa.eu.int/ comm/ internal_market/ en/dataprot/ inter/ priv.htm (last visited Mar. 9, 2003).

7. Sun Kyung Kwun Comparative Analysis of Protection of Personal Information: the U.S. and Korea, *at* http://www.cyberprivacy.or.kr (last visited Mar. 21, 2003).

8. United Nations (UN), Guidelines Concerning Computerized Personal Data Files (1990), *at* http://europa.eu.int/ comm/ internal_market/ en/ dataprot/ inter/ un.htm (last visited Mar.9, 2003).

9. Young Wha Jung, *Policy Measures for Protection of Privacy in Information Society*, Symposium Reports of Civil Activists Associates for Protection of Privacy 1 (2001), *at* http://www. privacy.or.kr/ privacy.text.htm (last visited Mar. 21, 2003).