THE TIGER ON THE PENINSULA IS DIGITIZED: KOREAN E-COMMERCE LAW AS A DRIVING FORCE IN THE WORLD'S MOST COMPUTER-SAVVY NATION

Stephen E. Blythe[*]

I. HISTORICAL BACKGROUND 576
A. *South Korea: The "Tiger" on the Peninsula* 577
B. *The World's Most Computer-Savvy Nation* 579
C. *Korean E-Commerce: Dramatic Growth* 580

II. OBJECTIVES OF THE ARTICLE 582

III. ELECTRONIC SIGNATURES 582
A. *The First Electronic Signature Law: Utah* 582
B. *Attributes of a Digital Signature System* 584

IV. KOREA'S FRAMEWORK ACT ON ELECTRONIC COMMERCE 586
A. *Electronic Messages* 587
B. *E-Commerce Security Issues: Consumer Protections* 590
C. *E-Commerce Policies and Strategies for Their Achievement* 593

[*] Ph.D. Candidate (Law), The University of Hong Kong; Ph.D. (Business Administration), University of Arkansas, 1979; J.D. *cum laude*, Texas Southern University, 1986; LL.M. (Int'l Bus. Law) University of Houston, 1992; LL.M. (Info. Tech. Law) *with distinction*, University of Strathclyde (Scotland), 2005. Attorney at Law, Texas and Oklahoma; C.P.A., Texas. The Author practiced solo (employment-discrimination litigation) in Houston, Texas, was affiliated with the Cheek Law Firm (insurance-defense litigation) in Oklahoma City, and has engaged in management consulting in China. Additionally, the Author has taught law, accounting, and management at twelve universities located in the United States, Africa, and the Middle East.

D. Increasing Participation in E-Commerce 596
E. The E-Commerce Mediation Committee 598
F. Application to Foreign Persons or Entities 601

V. KOREA'S DIGITAL SIGNATURE ACT 601
A. Goals of the DSA 601
B. Selected Definitions 602
C. Legal Recognition of Certified Digital Signatures ... 603
D. The Regulation of Certification Authorities 603
E. Certificates 611
F. Security and Reliability of the Certification Process 614
G. Governmental Adoption of Digital Signature Certification Policy 620
H. Criminal Offenses and Penalties 623

VI. E-COMMERCE TRANSACTIONS CONSUMER PROTECTION ACT 626
A. Purpose, Overlaps with Other Acts, and Selected Basic Definitions 626
B. Limitations and Precedence of the CPA 628
C. E-Commerce Transactions 629
D. Protection of Consumers' Rights and Interests 643
E. Inspection and Supervision 645
F. Corrections and Penal Surcharges 647
G. Criminal Violations 650

VII. SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS 653
A. Recent History of Korea 653
B. The "Tiger" on the Peninsula: Economic Growth, Computer Adeptness, and Rise of E-Commerce 654
C. Korean E-Commerce Law 654
D. Recommendation: It Is Time for the World's Most Computer-Savvy Nation to Address the Online Piracy Problem 659

ABSTRACT

South Korea has been classified as one of the Southeast Asian "Tigers" because of its high rate of economic growth during the past twenty-five years. One recent aspect of the economic growth has been the remarkable surge of e-commerce since 2000. During the next five years, South Korean e-commerce is expected to grow even more. One of the drivers of the e-commerce proliferation is the high degree of computer literacy among the South Korean people, facilitated by the fact that South Korea enjoys the greatest percentage of citizens with high-speed internet connection in the world. Another important driver of South Korean internet commerce—and the primary focus of this Article—is its e-commerce law.

The Framework Act on Electronic Commerce (ECA) of 1999, implemented by the Ministry of Commerce, Industry and Energy (MCIE), set the stage for electronic proliferation. The ECA recognizes the legal validity of several forms of electronic signatures, commensurate with the trend in global electronic signature law, and established basic consumer protections even at the earliest stage of South Korean e-commerce development. The Digital Signature Act (DSA) of 1999 is a companion statute to the ECA. The DSA focuses on one type of electronic signature—digital—and was implemented by the Ministry of Information and Communications (MIC). The MIC is responsible for licensing and regulating of Certification Authorities, the verifiers of the authenticity and integrity of digital signatures and the electronic records to which they are affixed. The DSA also establishes criminal penalties for the fraudulent use of digital signatures. While the ECA and the DSA are noteworthy, the E-Commerce Transactions Consumer Protection Act (CPA) of 2002 differentiates South Korean e-commerce law from the herd.

The CPA provides some of the best—if not the best—consumer protections for e-commerce transactions in the world.

The CPA is implemented by the Federal Trade Commission (FTC) and includes the imposition of criminal penalties for its violation. The CPA underwent a major overhaul in 2005 that will become effective on April 1, 2006. The CPA deserves to be considered as a model law for other nations to emulate as they develop their e-commerce law. South Korea is now ready to turn its attention to another pressing problem—online piracy of intellectual property.

I. HISTORICAL BACKGROUND

During much of the past millennium, the Korean Peninsula was ruled as a unified, autonomous kingdom. After Japan's victory in the Russo-Japanese War of 1905, the Japanese began to occupy parts of Korea, and within five years they had officially claimed all of Korea as a Japanese possession.[1] For the next thirty-six years, Japan controlled Korea.[2] This period had a strong influence on Korean culture, an impact that is felt to this day. At the end of World War II, the victorious powers divided Korea into two parts; the northern portion adopted a Communist government, and the southern portion became a republic.[3] On June 25, 1950, North Korean military forces attacked South Korea.[4] The Korean War pitted the North Korean aggressor, supported by Chinese troops, against South Korean forces supported by several nations' forces representing the United Nations, most notably those from the United States.[5]

The liberty and freedom now enjoyed by the Republic of South Korea was paid for in blood. The number of deaths occurring in the Korean War are grim statistics indeed: 547,000 South Korean civilians, 113,248 South Korean soldiers, 33,741 American soldiers, and 1,078 British soldiers.[6] Other countries also contributed troops to help the South Korean cause, and

---

1. U.S. CENTRAL INTELLIGENCE AGENCY, South Korea, CIA World Factbook (2006), http://www.cia.gov/cia/publications/factbook/geos/ks.html [hereinafter CIA, South Korea].

2. *Id*.

3. *Id*.

4. *Id*.

5. *Id*.

6. Matthew White, *Death Tolls for the Major Wars and Atrocities of the Twentieth Century*, http://users.erols.com/mwhite28/warstat2.htm (last visited Apr. 3, 2006).

their killed-in-action figures were significant: Turkey (720), Canada (310), France (290), Australia (269), Greece (170), Colombia (140), Ethiopia (120), Netherlands (110), Thailand (110), Belgium (100), and Philippines (90).[7] After three years of combat, the two sides signed an armistice that split the two Koreas at approximately the thirty-eighth parallel.[8] To this day, North Korea continues to have a communist government while South Korea has evolved into a full-fledged democracy.

A. South Korea: The "Tiger" on the Peninsula

In 1960, South Korea was a very poor country whose underdeveloped economy was comparable to some of the African nations.[9] After 1980, however, due to a high rate of foreign investment and other factors,[10] South Korea's economy took off,

---

7. *Id*. The Republic of South Korea—the entire nation—stands as a living memorial to all of those South Koreans, Americans, British, and others who sacrificed their lives on the altar of freedom for her. Some of the U.S. interventionist actions during the past sixty years may have been mistakes, but the interventions into South Korea and Vietnam were not. The example of South Korea is exactly what the United States had in mind when it intervened in Vietnam. The United States desired the Republic of South Vietnam to have the same opportunities as the Republic of South Korea enjoyed. Just because the United States failed in Vietnam does not mean the cause was devoid of honor. The 58,000 young Americans who died in Vietnam gave their lives for a noble cause. *Those who have known the great triumphs deserve their accolades. Almost as deserving are those who dared to dream great dreams*, *but fell short, while striving intrepidly*. Now, the United States has its hands full again in another difficult intervention. It is too early at the time of this writing to predict the outcome in Iraq. If the Shiites, Sunnis, and Kurds are somehow able to forge a coalition government with the three groups working together in mutual respect, Iraq could become a democratic beacon for the Middle East. On the other hand, if the three groups start a full-blown civil war and descend into the abyss, the situation could become catastrophic for everyone, including the United States and the world. Only Al Qaeda would win in that nightmare scenario.

8. CIA, South Korea, *supra* note 1.

9. *Id*.

10. *Id*. Foreign direct investment was, of course, an externally originating factor. The following internal factors were also significant in the economic development of South Korea, especially during the 1980s: (1) close relationships between business firms and the government; (2) "directed credit" from government agencies to business firms; (3) import restrictions; (4) government sponsorship of some industries; (5) good cooperation from labor organizations; (6) government encouragement of imports of raw materials and technology instead of imports of consumer goods; and (7) government emphasis on personal savings instead of personal consumption. *Id*.

and the nation experienced marked economic growth.[11] Due to its expanding economy, South Korea has often been referred to as one of the Southeast Asian "Tigers."[12] In 2004, South Korea—the Tiger on the Peninsula—was preparing to join the trillion dollar club of world economies, and was creating a Gross Domestic Product (GDP) per capita that was fourteen times that of North Korea.[13] The South Korean government has even bigger economic plans on the drawing board. The Ministry of Commerce, Industry and Energy (MCIE) intends for South Korea to become one of the world's top four industrial superpowers by the end of this decade, focusing on the "future

11. *Id*.; *see also* U.S. CENTRAL INTELLIGENCE AGENCY, North Korea, CIA World Factbook (2006) http://www.cia.gov/cia/publications/factbook/print/kn.html [hereinafter CIA, North Korea] (last visited Apr. 3, 2006) (explaining that meanwhile, North Korea's economy has been languishing, and it remains one of the poorest nations in the world). See *infra* note 13 for comparable statistics of North and South Korea. The long-range planners of South Korea need to be thinking of the day when the two Koreas will reunite—they probably are, although they don't advertise it. If reunification happens—and it probably will sooner than most people predict—the South Korean economic planners will need to develop an ingenious plan to meld the two economies. Overnight, South Korea would have access to an enormous amount of unskilled manual labor—what to do with so much unskilled labor, especially in a high-tech nation like South Korea? To an extent, the planners can look to the re-unification of West and East Germany for ideas on how to rejoin the two Koreas, but the German Model is not very analogous because North Korea is far worse off than East Germany was at the time of reunification. Another intriguing issue is what to do with the one-million man army of North Korea. Could it be successfully combined with the South Korean Army, or would that be far too large a military force for the new Republic of Korea to want to maintain? This is food for thought, indeed.

12. Investopedia, Tiger Economy, http://investopedia.com/terms/t/tigereconomy.asp (last visited Apr. 3, 2006). The others are Indonesia, Singapore, Malaysia, Thailand, and China. *Id*.

13. CIA, South Korea, *supra* note 1. If South Korea is characterized as a tiger, North Korea must be a sick kitten. *Compare* CIA, South Korea, *supra* note 1, *with* CIA, North Korea, *supra* note 11 (showing the juxtapositioned economic indices of South and North Korea). The comparison of economic indices is astonishing: GDP in 2005: S. Korea = $983.3 billion, N. Korea = $ 40 billion; GDP per capita in 2005: S. Korea = $20,300, N. Korea= $1,800; Electricity Consumption: S. Korea = 303.3 billion kWh (2003), N. Korea = 17.43 billion kWh (2003); Oil Consumption: S. Korea = 2.168 million bbl/day (2003), N. Korea = 25,000 bbl/day (2003 est.); Exports: S = $277.6 billion f.o.b. (2004 est.), N. Korea = $ 1.275 billion f.o.b. (2004 est.); Economic Aid: S. Korea (Donor, 2003) = $334 million, N. Korea (Recipient, 2004) = $118 million). *Id.* Statistics do not lie. What a dramatic tribute to the industriousness and ingenuity of the South Korean people and to the efficacy of the Free Enterprise System!

strategic industries" of digital electronics, electronic medical equipment, the bio industry, the environmental industry, and the aviation industry.[14]

B. The World's Most Computer-Savvy Nation

The Republic of South Korea (South Korea or Korea) may be the most computer-adept nation in the world. By 2003, almost sixty percent of the population—more than 26 million South Koreans—were regularly connecting to the internet.[15] South Korea leads the world in broadband penetration—the percentage of citizens with access to high-speed internet connections, which offer significantly faster downloading capability and computer efficiency.[16] At least seventy-five percent of all households in South Korea have these high-speed connections.[17] On a per capita basis, this is three times the comparable figure of broadband penetration in the United States.[18] Amazingly, more South Koreans probably have wireless

---

14. MINISTRY OF COMMERCE, INDUSTRY AND ENERGY, 2010 INDUSTRIAL VISION: EMERGE AS ONE OF THE WORLD'S TOP FOUR INDUSTRIAL SUPERPOWERS (2005), http://www.mocie.go.kr/ index.jsp (follow "English" hyperlink; then follow "Toward 2010" hyperlink; then follow "2010 Industrial Vision: Emerge as One of the World's Top Superpowers" hyperlink) (last visited Apr. 3, 2006); *see also* Chung Sun-gu, *Korea as 'King of Tech' is Ministry Ambition*, JOONGANG DAILY, Apr. 11, 2004, *available at* http://joongangdaily.joins.com/200404/11/20040411225249080990090609061.html. Furthermore, Mr. Chin Dae-je, Minister of Information and Communication, plans for South Korea to become a world leader in technology. *Id*. He has launched a campaign to implement the "839 Project," designed to work toward attainment of expertise in eight telecommunications services, three infrastructure components, and nine growth information technologies. *Id*.

15. NATIONAL COMPUTERIZATION AGENCY MINISTRY OF INFORMATION AND COMMUNICATION, 2003 WHITE PAPER INTERNET KOREA 25, http://www.nca.or.kr/ homepage/main/gonggi.nsf/ca0d3180381c9bdbc92568f8001ecb97/d0af489868c199f2c9256 d6b0006aabb/$FILE/white+paper+2003.pdf. [hereinafter 2003 WHITE PAPER]

16. Peter Lewis, *Broadband Wonderland*, FORTUNE, Sept. 20, 2004, *available at* http:money.cnn.com/magazines/fortune/fortune_archive/2004/09/20/381168/index.htm.

17. *Id.*

18. *Id.*; *see also* ORGANISATION FOR ECONOMIC COOPERATION AND DEVELOPMENT, OECD BROADBAND STATISTICS, Dec. 2004, http://www.oecd.org/document/60/0,2340, en_2825_ 495656_2496764_1_1_1_1,00.html. Furthermore, the OECD reports that, on average, there are more than twenty-four broadband subscribers for every one hundred persons (of all ages) in Korea. *Id*. This is more than twice the broadband penetration rate of the United States, which had slightly less than ten. *Id*.; *see also* Karlin Lillington,

internet connections than regular wired access.[19] By 2008, the South Korean government predicts that at least 39.5 million citizens—out of a total of 48.5 million—will have broadband-connected mobile handsets.[20] This is eighty-one percent of the population! Is there any doubt that South Korea is the world's most computer-savvy nation?

C. Korean E-Commerce: Dramatic Growth

During the past five years, South Korean e-commerce has grown at a fast pace. This was predictable, given the high per capita income of the country and the computer-adeptness of the population. In 2000, e-commerce sales were $430 billion. By 2004, that statistic was expected to balloon to $7 trillion,[21] a growth rate of 1,628%! Additionally, the e-commerce growth continues: South Korea's National Statistical Office reported that e-commerce in September of 2005 amounted to 947 billion won.[22] If annualized, that figure would amount to 11.3 trillion won.[23] In September 2005 alone, 107 more online marketing websites (cybermalls) came into existence.[24] What about the future of South Korean e-commerce? If you want a sanguine answer, just ask Meg Whitman, CEO of eBay, the largest online auction firm in the United States. Currently, eBay owns a sixty-

---

Korean Housewives Want Speedy Net, WIRED NEWS, Jan. 1, 2003, http://www.wired.com/news/infostructure/0,1377,56525, 00.html.

19. 2003 WHITE PAPER, *supra* note 15, at 27.

20. Lewis, *supra* note 16; Mun Y. Yi, *A Critical Look at Cyber Korea: Quantity vs. Quality*, *in* COOPERATION AND REFORM ON THE KOREAN PENINSULA 62 (2002) (stating that Koreans access the internet for entertainment far more than in the United States). But that is still not all. In Korea, almost eighty percent of all internet users access music and movies, about fifty-three percent of internet users play online games, and forty-one percent of internet users download files from the internet. *Id.* The comparable statistic for these forms of participation in the United States is only about twenty to thirty percent. *Id.* Unfortunately, as will be emphasized at the end of this Article, most of the Korean access to copyrighted materials is unauthorized, and this is the next important computer law issue that needs to be tackled by the Korean government.

21. Republic of Korea E-commerce, http://www.ecommerce.or.kr/about/ec_overview.asp (last visited Apr. 3, 2006).

22. Yahoo! Australia & NZ Finance, South Korea E-commerce Sales Surge in September, Nov. 7, 2005, http://au.biz.yahoo.com/051106/17/p/cp45.html.

23. *Id.*

24. *Id.*

two percent stake in Internet Auction, the largest internet auction firm in South Korea.[25] While visiting South Korea last year, Ms. Whitman reflected upon the immensity of South Korea's IT infrastructure and its high broadband penetration, and described Korea's e-commerce growth potential as "limitless."[26]

The attainment of such an impressive e-commerce growth was facilitated by the enactment of three important e-commerce statutes in South Korea:

(1) the Framework Act on Electronic Commerce (ECA) (amended 2002);
(2) the Digital Signature Act of 1999 (DSA) (amended 2002); and
(3) the Act on the Consumer Protection in the Electronic Commerce Transactions, etc. (CPA) (most recently amended in 2005, effective as of April 1, 2006).

Collectively, these statutes establish legal recognition of electronically negotiated contract, support the development of secure and reliable electronic payment systems, and create important rights and protections for e-commerce buyers.[27] Without these laws, e-commerce would have not been able to grow nearly as much. These statutes are the primary focus of this Article but not the only focus.

A future-oriented perspective is also needed. What should be the next evolutionary stage of internet law in Korea? The government of South Korea is committed to attainment of a strong global position in e-commerce.[28] In order for e-commerce

25. *Id.*

26. Kim Tae-gyu, *Korea's E-commerce Potential Limitless*, THE KOREA TIMES, Apr. 9, 2004, *available at* http://times.hankooki.com/lpage/biz/200404/kt2004040917514711910.htm.

27. Digital Signature Act No. 5792, *in* 16 STATUTES OF THE REPUBLIC OF KOREA 1219, art. 3(3) (Korean Legislation Research Institute 1999) [hereinafter DSA]; Framework Act on Electronic Commerce, *in* 13 STATUTES OF THE REPUBLIC OF KOREA 395 (Korean Legislation Research Institute 1999) [hereinafter ECA]; Act on the Consumer Protection in the Electronic Commerce Transactions, *in* 13 STATUTES OF THE REPUBLIC OF KOREA 481 (Korean Legislation Research Institute 1999) [hereinafter CPA].

28. Korea.net, Korea Committed to Global Promotion of E-commerce, Dec. 10, 2004, http://www.korea.net/News/News/NewsView.asp?serial_no20041209015.

growth to continue, it is necessary for internet law to evolve in a positive manner. That is another important focus of this Article: What should be the next focus of South Korean internet lawmakers?

II. OBJECTIVES OF THE ARTICLE

The objectives of this Article are as follows:

- to concisely cover the recent history of the Republic of South Korea and her high rate of economic growth during the past quarter-century;
- to present evidence that South Korea may be the most computer-adept nation in the world;
- to describe the high rate of growth of e-commerce currently underway in South Korea;
- to describe the basic aspects of public key infrastructure technology and digital signatures, and explain their impact on e-commerce transactions;
- to explain the significance of the ECA and its provision for legal recognition of electronic transactions;
- to describe the DSA and its requirements pertaining to CAs;
- to discuss how South Korea's CPA offers some of the best protections in the world for online buyers; and
- to make recommendations pertaining to the next direction in which Korean internet law should evolve.

III. ELECTRONIC SIGNATURES

A. The First Electronic Signature Law: Utah

In 1995, the State of Utah became the first jurisdiction in the world to enact an electronic signature law.[29] In that statute, Utah recognizes only digital signatures, rather than other types of electronic signatures.[30] Although such a law provides for

29. *See* 1998 A.B.A. SEC. BUS. L., http://www.abanet.org/buslaw/blt/8-2lock.html; *see also* UTAH CODE ANN. § 46-3-101 et seq. (1999).

30. UTAH CODE ANN. § 46-4-401; s*ee also* Jochen Zaremba, *International Electronic*

relatively more security in e-commerce transaction,[31] it carries the disadvantage of being too restrictive because it favors the digital signature to the exclusion of other forms of electronic signatures. A desire for heightened security seems to have been paramount to the drafters of the Utah statute. However, there are tradeoffs. The attainment of greater security, achieved by granting recognition only to the more sophisticated digital signature, means e-commerce participants' choices are limited. They are forced to use a technology that offers high security but one that perhaps is more expensive, less convenient, too complicated, and less adaptable to technologies employed by other nations.[32]

In drafting an e-commerce law for South Korea, legislators decided to give preference to the digital signature because it affords the greatest level of reliability and security.[33] Despite the fact that Korean legislators recognized the security advantages afforded by the relatively greater sophistication of the digital signature, they did not grant it a monopoly.[34] Other forms of electronic signatures may be employed.[35] This technological open-mindedness is commensurate with a global perspective and allows for e-commerce parties in South Korea to more easily

---

Transaction Contracts Between U.S. and E.U. Companies and Customers, 18 CONN. J. INT'L L. 479, 511 (2003) ("An electronic signature is defined as 'any letters, characters, or symbols manifested by electronic or similar means and executed or adopted by a party with the intent to authenticate a writing.'"). There are many forms of electronic signatures; examples include "a name typed at the end of an e-mail message, a digitized fingerprint, a digitized image of a handwritten signature that is attached to an electronic message, a retinal scan, a pin number, or a digital signature." *Id*.

31. *See* UTAH CODE ANN. § 46-4-401.

32. *See also* Sarah E. Roland, *The Uniform Electronic Signatures in Global and National Commerce Act: Removing Barriers to E-Commerce or Just Replacing Them with Privacy and Security Issues?* 35 SUFFOLK U. L. REV. 625, 638–45 (2001) (noting that it is debatable as to whether technological neutrality or technological specificity is the correct road to take).

33. *See* Stephen E. Blythe, *Digital Signature Law of the United Nations, European Union, United Kingdom and United States: Promotion of Growth in E-Commerce With Enhanced Security*, 11 RICH. J. L. & TECH. 2 (2005), *available at* http://law.richmond.edu/jolt/v11i2/article6.pdf (giving a concise treatment of the United Nations, European Union, British, and American laws regarding digital signatures).

34. DSA, *supra* note 27, art. 2.

35. *Id.*

negotiate electronic contracts with parties from other nations.[36]

B. Attributes of a Digital Signature System

It is appropriate at this point to consider some of the characteristics of a digital signature system. If the parties to an e-commerce transaction employ a digital signature, that decision will have the following effects:

- employment of an asymmetric cryptology;
- utilization of public key infrastructure (PKI); and
- interaction with a Certification Authority (CA).[37]

1. Asymmetric Cryptology

In order for a digital signature to attain the same legal status as an ink-on-paper signature, asymmetric key cryptology must have been employed in its production.[38] Such a system employs double keys—one key is used to encrypt the message by the sender, and a different, albeit mathematically-related,[39] key is used by the recipient to decrypt the message.[40] The sender has a private key, known only to him, used to generate the digital signature. [41] The recipient uses the public key, often available online, to verify that the proper party created the message and

---

36. *Id.* art. 27-2.

37. *See* Richard Wu, *Electronic Transaction Ordinance—Building a Legal Framework for E-commerce in Hong Kong,* J. INFO. L. & TECH. (2000), *available at* http://www2.warwick.ac.uk/ fac/soc/law/elj/jilt/2000_1/wu/.

38. Renard Francois, *Fair Warning, Preemption and Navigating the Bermuda Triangle of E-Sign, UETA, and State Digital Signature Laws*, 19 J. MARSHALL J. COMPUTER & INFO. L. 401, 405–06 (2001).

39. *PKI Assessment Guidelines*, 2001 ABA SEC. OF SCI. & TECH. LAW 301, *available at* http://www.abanet.org/scitech/ec/isc/pagv30.pdf.

40. *Id.*; *see also* Robin C. Capehart & Mark A. Starcher, *Wired, Wonderful West Virginia: Electronic Signatures in the Mountain State*, 104 W. VA. L. REV. 303, 311–12 (2002). By contrast, "symmetric" cryptology employs one key. *Id*. The same key is used for both encryption and decryption. *Id*. Thus, the sender and recipient are using the same key. *Id*. There are two disadvantages: (1) two stranger-parties using a public network have no way to securely transmit symmetrical keys to be used in subsequent transmissions; and (2) the transfer of a key in such a situation could possibly be intercepted or modified by a third party. *Id*.

41. *PKI Assessment Guidelines*, *supra* note 39, at 305.

that it has not been altered during transmission.[42] This is a very good system for e-commerce because two stranger-parties, perhaps living far apart, can confirm each other's identity and reduce the likelihood of fraud in the transaction.

2. Public Key Infrastructure

Before an individual can digitally sign anything, he must first possess a pair of keys—the private key and a related public key.[43] The individual applies to a CA to confirm his identity and to issue the pair of keys.[44] After the applicant's identity has been confirmed, the CA issues a certificate as verification of the subscriber's identity.[45] The certificate is placed in a public repository, most often the CAs website.[46] Whenever the subscriber digitally signs a message, the CA confirms the signature of the sender; whereupon, the CA informs the recipient of the encrypted message which "public key" is necessary to decode the message.[47] At that point, the recipient is able to access the public key which is used to decrypt the sender's message.[48]

3. Certification Authorities

South Korea does not have a compulsory system in its regulation of CAs.[49] CAs are not strictly required to have a

---

42. *Digital Signature Guideline: Legal Infrastructure for Certification, Authorities, and Secure Electronic Commerce*, 1996 ABA SEC. OF SCI. & TECH. LAW, 9–10, *available at* http://www.abanet.org/scitech/ec/isc/dsg.pdf.

43. Aristotle Mirzaian, *Electronic Commerce: This is Not Your Father's Oldsmobile*, 26 RUTGERS L. REC. 7 (2002), *available at* http://www.lawrecord.com (follow "Archives" hyperlink; then follow "Volume 26" hyperlink; then follow "Mirzaian" hyperlink).

44. Michael H. Dessent, *Digital Handshakes in Cyberspace Under E-Sign: 'There's A New Sheriff in Town*!, 35 U. RICH. L. REV. 943, 992 (2002).

45. *Id.*

46. *Id.*

47. *Id.*

48. Jane K. Winn, *The Emperor's New Clothes: The Shocking Truth About Digital Signatures and Internet Commerce*, 37 IDAHO L. REV. 353, 386 (2001).

49. DSA, *supra* note 27, art. 3(3); *see also* Stephen E. Blythe, *Hong Kong Electronic Signature Law and Certification Authority Regulations: Promoting E-Commerce in the World's 'Most Wired' City*, 7 N.C. J. L. & TECH. 1 (2005). Similarly, other jurisdictions (for example, Hong Kong) also use a voluntary regulatory program for their CAs. *Id*. at 9.

license in Korea to conduct CA activities. However, for CAs to be effective, subscribers, relying third parties, and the general public should trust and be willing to place reliance in the CA. The DSA helps to accomplish this in Korea by specifying stringent requirements for the issuance of the CA license. To qualify, the CA must be able to convince the Korean Ministry of Information and Communication (MIC) that it uses a trustworthy system of issuing and withdrawing certificates; displays them in a public repository; and is able to efficiently and effectively confirm the authenticity and integrity of digital signatures and the messages to which they are affixed.[50]

IV. KOREA'S FRAMEWORK ACT ON ELECTRONIC COMMERCE

The Framework Act on Electronic Commerce was originally enacted and implemented in 1999.[51] A wholly amended version of the ECA was enacted on January 19, 2002,[52] and it was implemented on July 1, 2002.[53] The federal governmental agency responsible for implementation of the ECA is the Ministry of

---

In voluntary systems, it is possible for a firm to engage in CA work without a license. *Id*. However, there are disadvantages in doing so, particularly the lack of official legal recognition given to the digital signatures they would certify, as well as the inability of an unlicensed CA to limit the liability of the firm. *Id*. Accordingly, there are no unlicensed CA's in Hong Kong, a jurisdiction with an ostensibly voluntary licensing program for CAs. *Cf. id.*; *see also* PRESIDENTIAL ORDER (NO. 18), LAW OF THE PEOPLE'S REPUBLIC OF CHINA ON ELECTRONIC SIGNATURE, art. 16 (2004), *available by subscription only at* http://www.lawinfochina.com/ dispecontent.asp?db=1&id=3691 (last visited Apr. 3, 2006) (showing that in Mainland China, there is compulsory licensing of CAs—no CA is allowed to operate without a license, and stringent sanctions are provided for imposter CAs operating without a license).

50. DSA, *supra* note 27, art. 4.

51. ECA, *supra* note 27. The Korean Legislation Research Institute (KLRI) is an independent nonprofit organization funded by the government of the Republic of South Korea. *Id.* The KLRI's charge is to translate all of the Korean federal statutes into English. *Id.* They do an admirable job of this and the *Statutes'* twenty volumes, in loose-leaf form, are continually updated. *Id.* This is one of the Korean government's globalization thrusts. Of course, the official statutes are the ones in Korean language as originally enacted. *Id.* However, given that the KLRI's work is financed by the Korean government, the English-language versions of the *Statutes* used in research for this Article could be described as *quasi*-official. *See id.*

52. *See id*. (explaining that the ECA was amended by Act No. 6614).

53. *Id*. (addenda).

Commerce, Industry and Energy.[54] The purpose of the ECA "is to contribute to the national economy by clarifying legal relations of the electronic commerce, ensuring its security and reliability, and creating the foundation for its promotion."[55] In the ECA, electronic commerce is defined as "any transaction of which the whole or part of goods or service is made through electronic messages in transacting goods or service."[56] The ECA applies to all e-commerce, unless it conflicts with other laws.[57]

A. Electronic Messages

1. Recognition of Electronic Form

The validity of a message will not be denied merely because it happens to be in electronic form, provided this does not conflict with other laws.[58]

2. Compliance with Retention Requirement

If another law mandates that documents be retained, the electronic form will be permissible to satisfy this requirement, provided the electronic document has the following characteristics:

- it is accessible;
- it is kept in the same form as when it was created, transmitted, or received, or this form may be reproduced; and
- it contains the name of the sender and receiver, and the dates of transmission and receipt.[59]

However, the part of the transmission that is created as a result of sending or receiving the message is not considered to be

---

54. *Id*. art. 39. The authority of the MCIE to implement the ECA is partially delegated to other agency heads or to heads of local government, according to the conditions that are specified in the Presidential Decree. *Id*. (A Presidential Decree is similar to a U.S. Executive Order.).

55. *Id*. art. 1.

56. *Id*. art. 2.

57. *Id*. art. 3.

58. *Id.* art. 4.

59. *Id.* art. 5(1).

a part of the electronic message.[60]

3. Time and Place of Sending and Receiving

Time Sent

The electronic message is deemed sent when the receiver inputs it into his computer and becomes capable of receiving the message.[61]

Time Received

The electronic message is considered to have been received when it enters the specific information processing system to which the receiver requested it be sent.[62] If the electronic message enters another information system, the applicable time is when the receiver removes it from the other system. Additionally, if the receiver has not designated a specific information system where the messages will be sent, the applicable time is when the message enters any information system under the control of the receiver.[63]

Place Sent/Received

The message will be considered to have been sent from the respective business place of the sender or receiver.[64] If there is more than one business place to consider, the message is deemed to have been sent from the business place that was primarily managing the electronic message. However, if the sender or receiver does not have a business place, the message is considered to have been sent from his habitual residence.[65]

60. *Id.* art. 5(2).
61. *Id.* art. 6(1).
62. *Id.* art. 6(2).
63. *Id*.
64. *Id.* art 6(3).
65. *Id.*

4. Situations in Which it is Assumed that the Message was Sent

In the following scenarios, the receiver may act upon the assumption that an electronic message contains a manifestation of will of the sender acting through his agent, or automatically, and using other electronic devices: (1) the receiver has used the pre-arranged procedure to verify that the message comes from the sender; or (2) the person who transmitted the message is reasonably believed by the receiver to have done so based on the will of the sender or his agent.[66] However, the assumption that the sender in question transmitted the message is not applicable when the receiver has notice from the sender that the message is not his own, or when the receiver becomes aware, or should have become aware, that the message did not originate from the sender.[67]

5. Assumption that Each Message is Independent

The receiving party has the right to assume that each electronic message is independent and does not have a relationship to other messages.[68] This assumption becomes inapplicable if the receiver fails to follow the verification procedure that has been previously agreed upon between the parties.[69]

6. Receiver's Confirmation

If the sender demands an acknowledgement of receipt from the receiver, the message is not considered to have been transmitted until the sender is receives the confirmation.[70] If the sender demands an acknowledgement of receipt from the receiver but fails to convey to the receiver that this is an absolute requirement, the sender is allowed to withdraw the message after the passage of a reasonable period of time.[71]

---

66. *Id.* art. 7(1)–(2).

67. *Id.* art. 7(3).

68. *See id.* art. 8.

69. *Id.*

70. *Id.* art. 9(1). In this situation, Article 534 of the Civil Act does not apply. *Id.*

71. *Id.* art. 9(2). If the sender has indicated a specific length of time, or if the

7. Alternate Agreements of Parties Allowed

The parties are to make their own agreement concerning the time and place of transmission and reception, the situation in which the sender is assumed to have sent the message, the assumption of independence of each message, and acknowledgement of receipt. If they do so, Articles 6 through 9 of the ECA become inapplicable.[72]

8. Electronic Transactions Act Does Not Cover Digital Signatures

Legal issues pertaining to digital signatures are considered in the Digital Signature Act,[73] and the Electronic Transactions Act does not apply to those issues.[74]

B. E-Commerce Security Issues: Consumer Protections

1. Confidentiality of Consumer Information

The government of the Republic of South Korea assumes responsibility for enacting laws that further the attainment of security and reliability in e-commerce transactions and protects the confidentiality of private information of e-commerce purchasers.[75] All e-commerce sellers and middlemen must observe all relevant information security laws, including the Act on Promotion of Information and Communications Network Utilization and Information Protection.[76]

2. Confidentiality of Trade Secrets

The government also assumes responsibility for the attainment of reliability and security in e-commerce so that business and corporate trade secrets are not divulged or leaked

---

parties have agreed to a specific length of time, then that length of time will apply. *Id.*

72. *Id.* art. 10.

73. *See generally* DSA, *supra* note 27.

74. ECA, *supra* note 27, art. 11.

75. *See id.* art. 12(1).

76. *Id.* art. 12(2).

to unauthorized parties.[77] E-commerce sellers, including their computer systems departments, must develop stringent policies designed to protect the user's business secrets.[78] Unauthorized disclosure of trade secrets is prohibited.[79]

3. Encryption Technology May Be Used

To gain security in e-commerce transactions, encryption technology may be used.[80]

4. Consumer-Protection Policies

Pursuant to the consumer protections established in other acts,[81] the government assumes responsibility for crafting consumer protections applicable to e-commerce purchasers. To that end, the government reserves the right to advise e-commerce firms (and any association of e-commerce firms) to draft a code of fair policies and practices to be implemented on a daily basis to their e-commerce sales. This should help to prevent the unfair treatment of customers or unfair business practices.[82]

5. Consumer Information and Grievances

The government assumes responsibility for ensuring that e-commerce buyers are well informed and educated about their rights and responsibilities.[83] Additionally, the government

77. *See id.* art. 13(1).

78. *See id.* art. 13(2).

79. *Id.* art. 13(3). Implementation measures of this section may be covered in a Presidential Decree. *Id.* art. 13(4).

80. *Id.* art. 14(1). However, the government may restrict the utilization of encryption technology (encoded products) if a national security issue is at stake. *Id* art. 14(2). In these situations, the government has the right of access to the encryption devices and to the "original text of encoded information." *Id.* Encryption is discussed in this Article; it is the foundation upon which digital signatures are based. *See* DSA, *supra* note 27.

81. ECA, *supra* note 27, art. 15(1). Insofar as the Consumer Protection Act and the Door-to-Door Sales Act pertain to consumers, these Acts have now been largely replaced by the Act on the Consumer Protection in the Electronic Commerce Transactions. *See infra* Part VI.

82. ECA, *supra* note 27, art. 15(2).

83. *Id.* art. 16(1).

recognizes the establishment of a grievance process for dealing with dissatisfied e-commerce consumers.[84]

6. Sellers' Responsibilities to Ensure Security and Reliability of E-Commerce

Firms selling products and services over the internet are expected to take measures designed to ensure the security and reliability in their relations with consumers, including but not limited to, the following:

- informing consumers of the firm's trade name and the name of corporate representative;
- providing consumers with accurate information relating to the goods and services offered and to the terms of the negotiated contract;
- utilizing of a standard contract and making it available to the buyer so that the buyer more easily understands its terms;
- establishing easy-to-use procedures enabling the buyer to cancel or alter the contract by herself;
- establishing procedures to promptly deal with matters pertaining to dissatisfied or disgruntled buyers;
- designing procedures so that the buyer can easily withdraw from the contract, return goods, or make an exchange; and
- creating rules requiring retention of documents for a reasonable period, so that all e-transactions can be referenced at a later time.[85]

7. Government Recognition of Excellent E-Commerce Firms

"The Government may support the authentication project for excellent business operator of electric commerce, to protect consumers and to ensure the sound development of business operators of electric commerce."[86]

---

84. *Id.* art. 16(2).

85. *Id.* art. 17.

86. *Id.* art. 18.

C. E-Commerce Policies and Strategies for Their Achievement

1. Basic Principles

The following are basic principles upon which the e-commerce policies are grounded:

- the use of private initiatives to accomplish e-commerce policies;
- minimal government regulation;
- the attainment of secure and reliable electronic transactions; and
- a high degree of international cooperation.[87]

2. Development and Implementation of Promotional Programs

Based upon the principles just enumerated, the following programs are pursued for e-commerce:

- fundamental management of the programs;
- achievement of international e-commerce norms;
- establishment of good electronic payment systems;
- protection of intellectual property rights;
- protection of the rights of all parties involved in e-commerce;
- enhancement of the reliability and security of e-commerce transactions;
- adoption of standard technologies in e-commerce;
- promotion of consumer participation and interest in e-commerce;
- international cooperation;
- facilitation of growth in e-commerce by facilitating the growth of its basic infrastructure;
- development and activation of broadband internet connections; and
- other items necessary for the proliferation of e-commerce.[88]

87. *Id.* art. 19.

88. *Id.* art. 20(1).

The directors of governmental agencies are responsible for development of programs that they are capable of carrying out and relate to the twelve categories of e-commerce programs previously mentioned. The directors take these new programs into account as they develop major policies for their respective agencies.[89]

The various programs developed by the several governmental agencies are coordinated by the MCIE through a central administrative agency. Furthermore, the Minister, in conjunction with the Committee on Electronic Commerce Policy (CECP), deliberates on proposed e-commerce policies. [90] Before implementing new policies, the Informatization Promotion Committee must approve them.[91]

3. Committee on Electronic Commerce Policy

The Committee on Electronic Commerce Policy, established by the MCIE, crafts policies pertaining to e-commerce promotion.[92] Specifically, the CECP considers the following categories of issues:

- promotional programs;
- evaluation of efficacy of promotion programs;
- coordination of the promotion policies or the programs carried out by the various agencies of the government; and
- other issues brought up by the Chairperson of the CECP.[93]

The CECP may consist of no more than thirty members. One of the members is the MCIE, who acts as the chairman for the CECP.[94] CECP will be chaired by the Minister of Commerce, Industry and Energy. The Minister appoints the other members, who must be public officials of Grade III or higher and have

89. *Id.* art. 20(2).

90. *Id.* art. 21.

91. *Id.* art. 20(3). The Informatization Promotion Committee was established by article 8 of the Framework Act on the Informatization Promotion. *See id.*

92. *Id.* art. 21(1).

93. *Id.* art. 21(2).

94. *Id.* art. 21(3).

duties or expertise relating to e-commerce.[95]

4. Korea Institute for Electronic Commerce

The ECA obligates the government of Korea to establish the Korea Institute for Electronic Commerce (KIEC). The goal of the KIEC is to encourage and facilitate the previously discussed e-commerce promotion projects and to do everything possible to establish governmental policies favoring the growth and development of e-commerce.[96] The legal status of the KIEC is that of a "juristic person."[97] The KIEC has the following specific duties:

- to conduct research pertaining to e-commerce firms and disseminate the results;
- to conduct research on e-commerce computer systems and the creation of a business environment conducive to their creation;
- conduct research concerning international standardization[98] of computer systems and diffusion systems;
- to carry out projects relating to technological development;[99]
- to carry out projects pertaining to management excellence in e-commerce firms;[100]
- to participate in international exchanges and programs of cooperation designed to promote e-commerce;[101]

95. *Id.*, art. 21(4). Additional details pertaining to the CECP's composition or duties may be added by Presidential Decree. *Id.* art. 21(5).

96. *Id.* art. 22(1). To fund its budget, the KIEC is authorized to engage in money-making projects; details may be provided by Presidential Decree. *Id.* art. 22(4). If these funds are insufficient to pay for its expenses, the KIEC may be entitled to a government subsidy. *Id.* art. 22(5). The KIEC may collect contributions from business firms engaged in e-commerce. *Id.* art. 22(6). The KIEC may also charge fees to persons its standards (under conditions described in a Presidential Decree). *Id.* art. 22(7).

97. *Id.* art. 22(2). Unless the ECA provides otherwise, the Civil Act's provisions pertaining to incorporated foundations apply *mutatis mutandis* to the KIEC. *Id.* art. 22(8).

98. *Id.* art. 24.

99. *Id.* art. 25.

100. *Id.* art. 18.

101. *Id*. art. 29.

- to manage the Korea Electronic Document Interchange Committee (EDIC);[102]
- to manage the Electronic Commerce Mediation Committee;[103] and
- to carry out other duties as assigned by the MCIE or the directors of the e-commerce-related central administrative agencies.[104]

D. Increasing Participation in E-Commerce

1. Technological Development

The government of Korea has adopted a policy that supports the continued growth of e-commerce activity throughout the country.[105] To determine how much e-commerce has grown, the MCIE may undertake appropriate statistical surveys.[106] To enable e-commerce parties inside South Korea to better interact with their counterparts outside South Korea, the government does everything it can to facilitate the usage of standard technologies that are in widespread global employment.[107] To that end, the Korea EDIC, which is established by the MCIE, conducts research on international standards for e-commerce.[108] The government may allow relevant institutes to act in its behalf, despite their nongovernmental status and may subsidize their expenses.[109] The government also fosters the following:

- technological standards for e-commerce;

---

102. *Id.* art. 24(2) (establishing the EDIC).

103. *Id*. art. 32 (creating the Electronic Commerce Mediation Committee).

104. *Id*. art. 22(3).

105. *See id*. art. 23.

106. *Id*. art. 28(1). In preparation of the statistical data, the rules laid out in the Statistics Act apply *mutatis mutandis*. *Id.* Additional details regarding the survey may be added by Presidential Decree. *Id*. art. 28(4). Furthermore, private business firms and government agencies involved in electronic transactions may be asked to respond to the survey. *Id*. art. 28(2). If these firms and agencies are asked, they must comply. *Id*. art. 28(3).

107. *Id*. art. 24(1).

108. *Id*. art. 24(2). Specific details pertaining to the work of this Committee may be added by Presidential Decree. *Id.*

109. *Id*. art. 24(3). The conditions for subsidization may be expressed by Presidential Decree. *Id.*

- technological cooperation and technological transfer;
- dissemination of information relating to e-commerce technology; and
- other matters pertinent to e-commerce technology.[110]

2. Personnel Development

Machinery, equipment, and technology alone are not enough; the most important e-commerce resource the government will promote is manpower.[111] To develop the necessary personnel for a thriving e-commerce, the government will do the following: (1) subsidize some or all of the expenses incurred by specialized institutes or universities in projects pertaining to e-commerce,[112] and (2) subsidize some or all of the expenses to specialized institutes or universities that are developing personnel with e-commerce expertise.[113]

3. E-Government

The government should lead the way in e-commerce development. Accordingly, federal, provincial, and local governments draft and implement programs designed to place their programs on an electronic footing.[114]

4. Internationalization Efforts

The government encourages cooperation and exchange of e-commerce information relating to technology, personnel development, standardization, and research.[115] Additionally, the Korean government fosters the advancement of its e-commerce into overseas markets.[116]

---

110. *Id*. art. 25.

111. *Id*. art. 26(1).

112. *Id*. art. 26(2). The Act on the Establishment, Operation, and Fosterage of Government-Invested Research Institutions (for institutes) and the Higher Education Act (for universities) govern subsidization. *Id.* Additional details regarding subsidization may be added by Presidential Decree. *Id*. art. 26(3).

113. *Id*. art. 26(2).

114. *Id*. art. 27.

115. *Id*. art. 29(1).

116. *Id*. art. 29(2).

5. Smaller Enterprises

Large entities are not the only focus of the government in the development of e-commerce. The government believes that medium-sized and small-sized organizations can compete successfully in the e-commerce arena, and government policies are designed to develop such competition.[117] The MCIE may create a special institution known as the Electronic Commerce Support Center (ECSC) focusing on e-commerce development in these smaller enterprises. The ECSC's mission would be to provide "education and training, technological guidance, information provision, management counseling, information provision, etc. related to electronic commerce . . . ."[118]

6. Tax Forgiveness as an Incentive

All levels of government (federal, provincial, and local) may grant tax relief to entities, either full or partial, to encourage them to pursue e-commerce activities. [119] The government may also give financial support to these entities. Government subsidization may be authorized if "any juristic person or organization" undertakes a project as part of an e-commerce promotion program.[120]

E. The E-Commerce Mediation Committee

To quickly and effectively deal with e-commerce disputes and reduce the amount of litigation that would otherwise come into existence, the ECA establishes an E-Commerce Mediation Committee.[121]

1. Qualifications of Mediators

The Mediation Committee consists of between fifteen and

117. *See id*. art. 30(1).

118. *Id*. art. 30(2). More specifics about this new organization may be provided by Presidential Decree. *Id*. art. 30(3).

119. *Id.* art. 31(1). The specific conditions for qualification for these tax benefits are part of the Restriction of Special Taxation Act and the Local Tax Act. *Id*. art. 31(1).

120. *Id*. art. 31(2).

121. *Id*. art. 32(1).

fifty members, and one of its members is also its chairperson.[122] The members work part-time for two year terms and may be re-appointed.[123] A secretariat within the KIEC[124] may be assigned to provide clerical help to the Mediation Committee.[125]

To qualify as a member of the Mediation Committee, an individual must be one of the following:

- current or former faculty members at a university or research institution in a field pertaining to e-commerce who holds, or have held, the rank of associate professor or higher;
- a current or former government official with "much experience" in e-commerce who holds, or has held, the rank of Grade IV or higher;
- a person qualified to serve as a judge, public prosecutor, or lawyer;
- a person recommended by a nonprofit organization that is listed in the Nonprofit Non-Governmental Organizations Act; or
- a person with significant knowledge relating to e-commerce and mediation.[126]

2. The Mediation Process[127]

Any person believing he has been wrongfully damaged in an e-commerce matter may apply to the Mediation Committee for mediation.[128] Within forty-five days of receipt of the application, the Committee will "prepare a plan for mediation" of the

122. *Id*. art. 32(2).

123. *Id*. art. 32(4).

124. *See id*. art. 32(5).

125. *Id*. art. 32(5).

126. *Id*. art. 32(3). Means of challenging the members' qualifications and procedures for their possible expulsion may be included by Presidential Decree. *Id*. art. 32(6).

127. In addition to the basic mediation procedures mentioned in Articles 33–37 of the ECA, more detailed procedural matters relating to the mediation process may be added by Presidential Decree. *Id*. art. 38.

128. *Id*. art. 33(1). The Mediation Committee may charge mediation participants for expenses incurred in the mediation process, as prescribed by Presidential Decree. *Id*. art. 37(1). Other expenses incurred by the Mediation Committee may be subsidized by the government. *Id*. art. 37(2).

dispute.[129] However, if the Committee needs more time, it should inform the parties, give the reasons for the delay, and tell them of the new timeframe.[130] Alternatively, to expedite the matter, the Committee may assign the dispute to a "mediation division" consisting of no more than three mediators.[131]

Similar to the requirements of a court of law, the Mediation Committee needs valid information on which to base its decision.[132] Accordingly, the Committee may order the parties to submit information. The parties must comply with the Committee's orders unless they have "justifiable reasons" for not doing so.[133] Additionally, the Committee may compel the parties to attend their meeting and listen to their opinion regarding the dispute.[134]

3. When a Final Protocol of Mediation Settlement is Justified

A Final Protocol of Mediation Settlement is justified in the following situations: (1) the parties agree with the mediation plan that the Mediation Committee has presented;[135] or (2) the parties have come together, negotiated, and made a settlement agreement among themselves.[136] In either of these situations, all parties must "sign and seal" the Final Protocol after it is prepared by the Mediation Committee.[137]

4. When a Final Protocol of Mediation is Not Justified

In the following situations, a Final Protocol is not justified:

- the application for mediation is withdrawn, or any of the parties to the dispute rejects mediation;
- any party to the dispute rejects the Committee's proposed

129. *Id*. art. 33(2).

130. *Id.*

131. *Id*. art. 33(3).

132. *Id*. art. 34(1).

133. *Id.*

134. *Id*. art. 34(2).

135. *Id*. art. 33(2).

136. *Id*. art. 35(1).

137. *Id*. art. 35(2). If the parties have formed the agreement themselves, the signed Protocol will have the same legal validity as their agreement. *Id*. art. 35(3).

plan of mediation;[138]

- any party to the dispute files a lawsuit pertaining to the matter; or
- the Committee considers mediation inappropriate "in view of the nature of the case."[139]

F. Application to Foreign Persons or Entities

The ECA has reciprocal application to foreign persons or entities participating in e-commerce with South Korean persons or entities.[140] The ECA applies to and protects foreign parties engaged in e-commerce transactions with Korean parties, with this proviso: the ECA will not apply to foreign parties if those foreign nations do not offer similar protections to Koreans engaged in e-commerce.[141]

V. KOREA'S DIGITAL SIGNATURE ACT

The Digital Signature Act[142] was enacted on February 5, 1999[143] and was implemented on July 1, 1999.[144]

A. Goals of the DSA

The ultimate goal for enacting the DSA was to advance "social benefit and convenience" through a reliable and secure framework for digital signatures.[145] Establishing such a framework will result in a greater utilization of digital signatures, thereby increasing utilization of electronic messaging and communication on a national level.[146]

---

138. *Id*. art. 33(2).

139. *Id*. art. 36.

140. *Id*. art. 40.

141. *Id*.

142. DSA, *supra* note 27.

143. *Id*. The DSA has been amended two times since its enactment: (1) Act No. 6360 of Jan. 16, 2001; and (2) Act. No. 6585 of Dec. 31, 2001. *Id.*

144. *Id*.

145. *Id*. art. 1.

146. *Id.*

B. Selected Definitions

The DSA includes some important definitions that deserve special attention:[147]

- Certified Digital Signature (CDS): Information in digital form combined with, or affixed on, an electronic message for the purpose of identification of the signer and verification that the message has been signed by that person.[148] Furthermore, it must be supported by a Certificate issued by a Licensed Certification Authority (LCA),[149] and have the following characteristics:
    - only the subscriber holds and knows the private key;
    - only the subscriber holds the private key at time of signing;
    - if either the digital signature (DS) or the message to which it is affixed has been modified since the signing, the subscriber is capable of becoming aware of the modification.[150]
- Digital Signature Creating Key (Private Key): a sequence of bits used to attach a DS to an electronic message;[151]
- Digital Signature Verifying Key (Public Key): a sequence of bits used to confirm the authenticity of a DS.[152]
- Certification: the act of confirmation that the private key is known only to, and is under the control of, the subscriber.[153]
- Authorized Certificate (Certificate): a computer record that confirms that the private key is known only to, and

147. *Id.* art. 2. Other words or phrases defined in Article 2 of the DSA include the following: electronic document, certificate (this was combined with the definition of "authorized certificate"), accredited certification practice, signatory, and personal data. *Id.*

148. *Id.* art. 2(2)–(3).

149. *See id*. art. 2(3).

150. *Id.* art. 2(2)–(3).

151. *Id.* art. 2(4).

152. *Id.* art. 2(5).

153. *Id*. art. 2(6).

is under the control of, the subscriber. Furthermore, it must have been issued by a LCA under Article 15 of the DSA.[154]

- Licensed Certification Authority (LCA): an entity existing under Article 4 of the DSA and engaged in the business of offering certification services to the public.[155]
- Subscriber: a person holding a private key that has been confirmed by a LCA.[156]

C. Legal Recognition of Certified Digital Signatures

In the past, a paper document was afforded legal recognition if it contained the following: a handwritten signature, a signature with a seal, or the person's name with a seal.[157] The DSA gives an electronic document with an affixed CDS the same legal status as these traditional signatures.[158] In the case of an electronic document with a CDS affixed to it, there are two legal presumptions: (1) the digital signature is the signature, signature and seal, or name and seal of the party in question; and (2) the message has not been tampered with since it was digitally signed.[159]

The DSA does not prohibit the use of uncertified digital signatures.[160] The contracting parties are free to use uncertified digital signatures.[161] If they do, they will have whatever effect that is agreed upon between the parties.[162]

D. The Regulation of Certification Authorities

The MIC is entrusted with the responsibilities of licensure and regulation of LCAs.[163]

---

154. *Id.* art. 2(7), (8).

155. *Id.* art. 2(10).

156. *Id.* art. 2(11).

157. *Id.* art. 3(1).

158. *Id*. art. 3(1). Note, however, that this legal recognition is only given if the digital signature is certified, meaning it is supported by a certificate issued by a CA. *Id.*

159. *Id.* art. 3(2).

160. *See id.* art. 3(3).

161. *See id.*

162. *Id*. South Korea uses a voluntary CA system, not a compulsory one. *Id.*

163. *Id*. art. 4(1). The MIC is authorized to delegate responsibilities to other

1. Qualifications of the Applicant for a LCA License

To be considered for a LCA license, an applicant must be a governmental agency, a local government, or a corporation; individuals are not qualified. [164] The prospective LCA must be able to show evidence to the MIC that they are able to perform LCA activities reliably and securely.[165] Accordingly, specific requirements must be met pertaining to technical abilities, financial status, work site, computer equipment, and other matters.[166]

No LCA license will be issued to any corporation having an officer(s) who is:

- legally incompetent or quasi-incompetent;
- legally bankrupt and has not been reinstated by the court;
- a criminal convict released from prison less than two years ago;
- a criminal convict presently serving a suspended sentence in lieu of imprisonment;
- disqualified due to a court decision or under another Act; or
- a former officer of a LCA organization whose license was revoked less than two years ago.[167]

Furthermore, a corporation whose license is revoked cannot apply for a new license until two years have passed since its revocation.[168]

2. The Certification Practice Statement

Before a LCA can open its doors for business, it must prepare a Certification Practice Statement (CPS) and present it

---

subordinate agencies if a Presidential Decree (executive order) so directs. *Id*, art. 30.

164. *Id.* art. 4(2).

165. *Id.* art. 4(1).

166. *Id*. art. 4(3). Other specific requirements are included in the DSA implementation regulations. *Id.* art. 4(4).

167. *Id*. art. 5(1); *see also id*. art. 12 (discussing suspension and revocation of certification).

168. *Id.* art. 5(2).

to the MIC for review and approval.[169] The CPS represents a detailed listing of the policies, procedures, and rules the LCA expects to follow in the conduct of its business.[170] The CPS must include the following matters:

- the types of certification work in which the LCA plans to engage;
- detailed methods and procedures to be employed in carrying out each type of certification work;
- specific items pertaining to its subscribers, such as the fees to be charged for its services, the rights and responsibilities of the subscribers, and the rights of responsibilities of the LCA; and
- other items that may be pertinent to the LCA's activities.[171]

The LCA has the duty to promptly report to MIC any changes that have been made to the CPS.[172] The MIC will then review the CPS.[173] If the MIC believes that any parts of the CPS pose a threat to the reliability and security of the LCA's work, or the MIC believes that any part may be detrimental to subscribers, the MIC may order the LCA to make necessary changes to the CPS within a fixed time period.[174] The LCA is expected to adhere to those policies, procedures and rules adopted in its CPS.[175]

3. Operational Aspects of the LCA

No Discrimination

The LCA is not allowed to discriminate in provision of services to subscribers and relying third parties based on race, gender, religion, national origin, or other unjustifiable reason.[176]

169. *Id.* art. 6(1).
170. *Id.*
171. *Id.*
172. *Id*. art. 6(2).
173. *Id.* art. 6(3).
174. *Id.*
175. *Id.* art. 6(4).
176. *Id.* art. 7(2).

Accordingly, the LCA is not allowed to refuse service to any party unless a compelling reason exists.[177]

Code of Practice

The MIC reserves the right to draft detailed procedures to be followed by LCAs pertaining to the certification of digital signatures.[178] The MIC will publicly announce these procedures.[179]

Acquisition or Merger of LCAs

The MIC must be informed if a LCA desires to purchase or merge with another LCA.[180] The specific information to be conveyed is prescribed in the Ordinance of the MIC.[181] The purchaser of another LCA, or the surviving corporation in the case of a merger, shall assume the responsibilities of the former LCA.[182]

Suspension or Closure of LCA Activities

If a LCA desires to temporarily suspend part or all of its work, both the MIC and subscribers must be informed at least thirty days in advance.[183] The suspension period may not exceed six months.[184]

If a LCA desires to go out of business, both the MIC and subscribers must be informed at least sixty days in advance.[185] In the event of closure of the business, all records, including valid, suspended, and revoked certificates must be transferred to another LCA. However, if the records cannot be transferred to the other LCA "due to unavoidable circumstances," the

177. *Id*. art. 7(1).

178. *Id*. art. 8. In the U.S. and Hong Kong, these meticulous guidelines are referred to as the "Code of Practice." For an example of how complicated these guidelines can be, *see* Blythe, *supra* note 33.

179. DSA, *supra* note 27, art. 8.

180. *Id.* art. 9(1).

181. *Id.*

182. *Id.* art. 9(2).

183. *Id*. art. 10(1).

184. *Id.*

185. *Id.* art. 10(2).

departing LCA must report this to the MIC.[186] Additionally, the MIC may order the Korea Information Security Agency (KISA)[187] to take control of the records and certificates from the departing LCA.[188] The Ordinance of the MIC contains more specific and detailed procedures and requirements pertaining to suspension or closure.[189]

Grounds for MIC's Issuance of Corrective Order

The following examples are potential grounds for the MIC to issue a corrective order to a LCA, requiring the LCA to take "corrective measures" by a certain deadline:[190]

- the performance of the LCA's work in such an improper manner that the security and reliability of the digital signatures is jeopardized;[191]
- the LCA fails to continue to met the licensing requirements that it meet when it was first licensed;[192]
- an officer of the LCA incurs one of the conditions specified in Article 5(1) of the DSA.[193]
- the LCA fails to file a required report, including a report of modifications,[194] with the MIC; or the LCA fails to abide by its own rules pertaining to the issuance of certificates, which are published in the CPS;[195]
- the LCA discriminates against subscribers, relies upon third parties for an unlawful reason, or refuses to provide

186. *Id.* art. 10(3).

187. Established under Article 52 of the Act on Promotion of Information and Communications Network Utilization and Information Protection. COMMITTEE FOR INFORMATION, COMPUTER AND COMMUNICATIONS POLICY, ORGANISATION DE COOPÉRATION ET DE DÉVELOPPEMENT ECONOMIQUES, WORKING PARTY ON INFORMATION SECURITY AND PRIVACY 35 (2005), http://www.oecd.org/ dataoecd/16/27/35884541.pdf.

188. DSA, *supra* note 27, art. 10(4).

189. *Id.* art. 10(5).

190. *Id*. art. 11.

191. *Id.* art. 11(1).

192. *Id.* art. 11(2). These requirements are specified in the procedures referenced in Article 4(3) of the DSA. *Id.* art. 4(3)

193. *Id.* art. 11(3). These include a state of bankruptcy and others. *See id*. art. 5(1).

194. *See id.* art. 6.

195. *Id.* art. 11(4).

service for an unlawful reason;[196]

- the LCA fails to abide by the specific guidelines drafted by the MIC pertaining to the issuance of certificates.[197]
- the LCA fails to file a required report with the MIC pertaining to an acquisition or a merger with another LCA;[198]
- the LCA does not inform the MIC, or file a report with it, concerning the suspension or closure of its business, or the LCA going out of business fails to transfer its records and certificates to another LCA;[199]
- the LCA whose license has been revoked does not transfer its records and certificates to another LCA, or the LCA fails to make a report to the MIC if there is no transfer;[200]
- the LCA does not provide to the MIC documents which are necessary in the execution of the MIC's oversight function;[201]
- the LCA either fails to suspend or reinstate a certificate when it has a duty to do so,[202] or the LCA does not ensure that information pertaining to the validity of a certificate is available to the general public at all times.[203]
- the LCA fails to revoke a certificate when it has a duty to do so,[204] or the LCA does not ensure that information pertaining to the revocation of a certificate is available to the general public at all times;[205] or
- the LCA does not adopt and execute "protective

196. *Id.* art. 11(5); *id.* art. 7 (stating the antidiscrimination provision).

197. *Id.* art. 11(5-2). In other jurisdictions, these are often referred to as the Code of Practice.

198. DSA, *supra* note 27, art. 11(6); *see also id*. art. 9(1) (describing reports the LCAs are required to submit).

199. *Id.* art. 11(7); *see also id.* art. 10 (specifying these requirements).

200. *Id.* art. 11(8); *see also id.* art. 12(2) (discussing revocation requirements).

201. *Id.* art. 11(9); *see also id.* art. 14(1) (referencing documents a LCA must submit to the MIC).

202 *Id.* art. 11(10).

203 *Id.* This duty of the LCA is laid out in Article 17 of the DSA. *Id.* art. 17.

204. *Id.* art. 11(11).

205. *Id.*; *see also id.* art. 18 (stating the LCA's duty of care).

measures" to provide security over the LCA worksite.[206]

Grounds for Mandatory Revocation of the LCA's License

The LCA's license will be revoked in either of the following two situations:[207] (1) the LCA's license was obtained through fraud or other illegal means;[208] or (2) if the LCA fails to obey the order of the MIC to suspend its LCA activities.[209]

The LCA whose license has been revoked must transfer its records (including all valid, suspended and revoked certificates) to another LCA.[210] However, if such a transfer is impossible due to "inevitable circumstances," this must be immediately reported to the MIC.[211]

Grounds for Suspension or Revocation

In the following three situations, the MIC may either suspend the LCA's license for a period not exceeding six months or revoke the LCA's license entirely:[212]

(1) the LCA did not begin to offer certification services within six months of being licensed, or the LCA ceases to provide certification services for at least six months;[213]
(2) the MIC orders the LCA to modify its CPS,[214] but the LCA fails to obey the order;[215] or
(3) the MIC issues a corrective order[216] to the LCA, but the LCA fails to obey the order without justification.[217]

206. *Id.* art. 11(11-2); *see also id.* art. 18-3.
207. *Id.* art. 12(1).
208. *Id.* art. 12(1)(1).
209. *Id.* art. 12(1)(2).
210. *Id.* art. 12(2).
211. *Id.* art. 12(2).
212. *Id.* art. 12(1).
213. *Id.* art. 12(1)(3).
214. *See id.* art. 6(3).
215. *Id.* art. 12(1)(4).
216. *See id.* art. 11.
217. *Id.* art. 12(1)(5).

Revocation: Automatic Takeover of LCA's Records

If the LCA's license is revoked, Article 10(4) of the DSA applies.[218] Under Article 10(4) the KISA obtains possession of the LCA's records and certificates.[219]

MIC Ordinance is Determinative of Procedures

Before revocation of the LCA's license, the MIC is required to give the LCA a hearing.[220] Other procedures and standards for suspension or revocation are contained in the MIC Ordinance.[221]

Alternative Punishment in lieu of Suspension: Fines

If the MIC determines that the suspension of the LCA's license would pose too stringent a burden on the LCA's subscribers and relying third parties or "may be harmful to other public interests," the MIC may impose a fine—referred to as a "penalty surcharge"—on the LCA.[222] The fine shall not exceed 20 million won.[223] The specific amount of the fine is determined on a case-by-case basis using the standards in the MIC Ordinance.[224] If a LCA is ordered to pay a fine by a certain date but fails to do so, the MIC shall commence a collection action based upon the law regarding "dispositions on default of national taxes."[225]

The MIC May Inspect the LCA

If the MIC deems it necessary for a certain LCA to maintain the security and reliability of certificates it issues, the MIC may compel the LCA to present requested documentary materials.[226]

---

218. *Id.* art. 12(3).

219. *Id.*

220. *Id.* art. 29.

221. *Id.* art. 12(4).

222. *Id.* art. 13(1).

223. *Id.* Twenty million *won* is approximately U.S. $ 20,559. Nytimes.com, Currency Converter, http://marketwatch.nytimes.com/custom/nyt-com/html-usmarkets.asp (last visited Apr. 3, 2006) [hereinafter Currency Converter].

224. DSA, *supra* note 27, art. 13(2).

225. *Id.* art. 13(3).

226. *Id.* art. 14(1).

Furthermore, if deemed necessary, the MIC may conduct a physical inspection of the LCA's worksite, [227] accounting books, records, computer equipment, and other facilities.[228] If the inspection occurs, the MIC official must present his identification card or badge at the beginning of the inspection visit.[229]

E. Certificates

1. Application for a Certificate

To be considered for a certificate, a person must apply to a LCA.[230] As a general rule, the LCA is expected to issue a certificate to those who submit an application[231] and pay the required fee.[232] However, the LCA must check the identification of each and every applicant for a certificate.[233] This is imperative and cannot be over-emphasized. If there is doubt about the applicant's identity, the LCA should not issue the certificate.

2. Information on the Certificate

If the person's application is in order and the certificate is issued, then the applicant assumes the status of one of the LCA's subscribers. A certificate must contain the following information:[234]

- the name of the subscriber (individual person's name or name of the entity);[235]

---

227. *Id.* South Korean law seems to regard the inspection as an extraordinary event. By comparison, Chinese law requires governmental supervision and inspection of LCAs. Order (No. 18) of the President of the People's Republic of China, Art. 25.

228. DSA, *supra* note 27, art. 14(1).

229. *Id.* art. 14(2). The DSA does not indicate whether the inspection will be unannounced or announced in advance. *Id.*

230. *Id.* art. 15(1).

231. *Id.*

232. *Id.* art. 28.

233. *Id.* art. 15(6) (listing procedures for verification of the identity of the applicant are determined by the MIC Ordinance).

234. *Id*. art. 15(2).

235. *Id*. art. 15(2)(1).

- the subscriber's "verifying key;"[236]
- the algorithm used by the subscriber and the LCA to sign the certificate;[237]
- a serial number;[238]
- the period of validity of the certificate;[239]
- the name of the LCA and other information that can be used to confirm the identity of the LCA;[240]
- if applicable, any limitations on the scope of use of the certificate;[241]
- if applicable, a statement that the subscriber is serving as a proxy for another party, and also, if desired by the subscriber, the "professional title" of the subscriber;[242] and
- a verification mark.[243]

3. Situations in Which the Certificate is Definitely No Longer Valid

In the following situations, the certificate will no longer be valid:[244]

- the certificate's period of validity expires;[245]
- the issuing LCA's license is revoked;[246]
- the certificate's validity has been suspended;[247] and

---

236. *Id*. art. 15(2)(2). This is the public key.

237. *Id*. art. 15(2)(3).

238. *Id*. art. 15(2)(4).

239. *Id*. art. 15(2)(5). Issues to be taken into account by the LCA in determination of the length of the period of validity include: (1) the purpose(s) of the certificate; (2) the scope of the certificate's uses; and (3) the security and reliability of the "computing techniques used for its issuance." *Id*. art. 15(5).

240. *Id*. art. 15(2)(6). Procedures to be followed in the ascertainment of the validity of an applicant will be specified in the Ordinance of the MIC. *Id*. art. 15(6).

241. *Id*. art. 15(2)(7); *see also id*. art. 15(4) (discussing when limitations on the scope or use of the certificate are allowed).

242. *Id*. art. 15(2)(8).

243. *Id*. art. 15(2)(9).

244. *Id*. art. 16(1).

245. *Id*. art. 16(1)(1).

246. *Id*. art. 16(1)(2); *see also id.* art. 12(1) (noting when a LCA's license shall be revoked).

247. *Id.* art. 16(1)(3); *see also id.* art. 17 (noting when a certificate shall be

- the certificate has been revoked.[248]

4. Situations in Which the Certificate May No Longer Be Valid

In the following situations, the MIC may suspend the validity of the certificates where the security and reliability of the certification are in jeopardy:[249] (1) the issuing LCA temporarily or permanently ceases its operations;[250] and (2) the issuing LCA's operations have been suspended[251] or revoked.[252] In either of these two situations, where the MIC decides to suspend the certificates' validity, the KISA will be advised and directed to immediately seize the certificates and take whatever steps are necessary to ensure that the information on the certificates continues to be accessible to all concerned parties.[253]

5. Grounds for a LCA to Suspend a Certificate

The LCA must suspend the validity of a certificate whenever the subscriber (or agent) so requests.[254] In that case, the subscriber will have six months in which to request that the validity be reinstated.[255] Whenever the LCA has suspended or reinstated the validity, pursuant to the just aforementioned sentences, relying third parties must be kept informed.[256]

6. Grounds for a LCA to Revoke a Certificate

In the following situations, the LCA is required to revoke

---

suspended).

248. *Id.* art. 16(1)(4); *see also id.* art. 18 (noting when a certificate shall be revoked).

249. *Id.* art. 16(2).

250. *Id.*; *see also id.* art. 10 (noting how cessation of operations is controlled).

251. *Id.* art. 16(2); *see also id.* art. 12 (discussing how the MIC controls suspension of a LCA's activities).

252. *Id.* art. 16(3); *see also id.* art. 12(1) (discussing how the MIC controls revocation of a LCA's activities).

253. *Id.* art. 16(3).

254. *Id.* art. 17(1).

255. *Id*.

256. *Id*. art. 17(2).

the certificate:[257]

- when the subscriber (or agent) requests the revocation;[258]
- the LCA learns that the certificate was procured through "fraud or other wrongful methods;"[259]
- the LCA learns that a subscriber
  - is deceased;
  - due to disappearance, has been declared legally dead by a court order; or
  - if a corporation, has been legally dissolved by a court order;[260] or
- the LCA learns that the security of the subscriber's private key has been compromised (for example, lost, stolen, or disclosed to a third party).[261]

When revocation occurs due to any of these four situations, the LCA must post that information on its website and take all reasonable actions to apprise the general public.[262]

7. Use of Certificate as a Form of I.D.

A person may use a certificate as a form of self-identification unless that is proscribed by any other law.[263]

F. Security and Reliability of the Certification Process

To protect its certification facilities, the LCA is responsible for the implementation of security measures as directed by the MIC.[264] The LCA must never lose sight of the fact that it is liable for damages incurred by subscribers or relying third parties, unless damages are caused by a force majeure or it is confirmed there was no negligence. [265]

257. *Id*. art. 18(1).

258. *Id*. art. 18(1)(1).

259. *Id*. art. 18(1)(2).

260. *Id*. art. 18(1)(3).

261. *Id*. art. 18(1)(4).

262. *Id*. art. 18(2).

263. *Id*. art. 18-2.

264. *Id*. art. 18-3.

265. *Id*. art. 26. To maintain quality control over the LCA's work, the MIC adopts a complaint filing procedure for the benefit of injured subscribers and relying third parties.

1. Operation of Certification System[266]

LCA's Duty of Security Over Worksite

To maintain the general public's confidence in the validity of certificates, the LCA must do everything possible to ensure the reliability and security of its certification facilities and equipment.[267]

Periodic Inspections

The MIC reserves the right to conduct inspections on a regular basis to ensure the reliable and secure operation of the LCA's facilities and equipment.[268]

Replacement of Facilities and Equipment

The LCA must promptly inform the MIC of any changes in its facilities or equipment. In such a case, the MIC may order the Information Security Agency to inspect the new items for any possible security deficiencies.[269]

2. Time-Stamping

If any subscriber or relying third party requests the LCA to time-stamp an electronic document, the LCA must do so.[270]

3. Maintaining Security Over the Private Key

Subscriber's Private Key

The subscriber must exercise control over the private key.[271] If it is lost, mislaid, stolen, disclosed to a third party, or is in jeopardy of being compromised, both the LCA and the relying

---

Id. art. 27(1).

266. *Id*. art. 19.

267. *Id*. art. 19(1).

268. *Id*. art. 19(2).

269. *Id*. art. 19(3).

270. *Id*. art. 20.

271. *Id.* art. 21(1).

third parties must be informed at once.[272] The LCA must provide subscribers with a "computational device" used to notify them of the fact the fact that the private key's security has been compromised.[273]

The LCA may not hold the subscriber's private key unless requested to do so by the subscriber.[274] If the LCA holds the private key by virtue of the subscriber's request, the LCA cannot use the private key or disclose the private key to a third party.[275]

LCA's Private Key

The LCA must maintain security over its own digital-signature-creating key. If the LCA's security is compromised, the LCA must immediately inform the Korea ISA of the compromise, and the Korea ISA must take actions to ensure reliability and security of its certification activities.[276]

4. Record-Keeping

The LCA maintains records pertaining to its issued certificates and maintenance of security of its certification activities.[277] The LCA must maintain these certificates for ten years after the certificates are no longer valid.[278]

5. Certificates: Control Issues[279]

The LCA and subscribers are required to keep information

272. *Id.*

273. *Id.* art. 21(2).

274. *Id.* art. 21(3).

275. *Id.* art. 21(3).

276. *Id*. art. 21(4).

277. *Id*. art. 22(1).

278. *Id*. art. 22(2). The duration of the retention period varies from jurisdiction to jurisdiction. For example, in Hong Kong the duration is seven years; in China, it is five years. THE GOVERNMENT OF THE HONG KONG SPECIAL ADMINISTRATIVE REGION, OFFICE OF THE GOVERNMENT CHIEF ADMINISTRATIVE REGION, CODE OF PRACTICE FOR RECOGNIZED CERTIFICATION AUTHORITIES PUBLISHED BY THE GOVERNMENT CHIEF INFORMATION OFFICER UNDER SECTION 33 OF THE ELECTRONIC TRANSACTIONS ORDINANCE (CAP. 553) 7, § 3.5 (Dec. 2004), *available at* http://www.ogcio.gov.hk/eng/caro/cop_pdf/cop.pdf; Order (No. 18) of the President of the People's Republic of China, Art. 24.

279. DSA, *supra* note 27,. art. 22-2.

in the certificate up-to-date.[280] The certificate includes the following information:

- name of the LCA and other information used to verify the LCA's identity;
- the fact that the subscriber controlled the digital-signature-creating-key at the time the certificate was issued; and
- the fact that the digital-signature-creating-key was valid at the time of the issuance of the certificate.[281]

Additionally, the LCA should provide the subscriber with a method of conveniently determining the following information:

- means of identification of the signer of the digital certificate;
- any limitations on the purpose, use, or permissible amount pertaining to the certificate or the digital-signature-creating-key; and
- any limitations on the scope of the LCA's liabilities.[282]

6. Infractions Using Others' Private Keys

Using another person's private key or disclosing it without authorization is a wrongful act.[283] It is also a wrongful act to possess another person's private key without authorization of that person, or to engage in acts that facilitate the issuance of a private key of another person, without authorization.[284] Similarly, it is a wrongful act to use a similar mark or other means for the purpose of misleading others into believing that an unauthorized certificate is actually authorized.[285]

7. Confidentiality of Private Information[286]

The LCA must protect the security of private information of its subscribers and other parties that it encounters in the

280. *Id*. art. 22-2(1).
281. *Id*. art. 22-2(2).
282. *Id*. art. 22-2(3).
283. *Id*. art. 23(1).
284. *Id*. art. 23(2).
285. *Id*. art. 23(3).
286. *Id*. art. 24.

performance of its certification work.[287] The confidentiality requirements imposed by the Act on Promotion of Information and Communications Network Utilization and Information Protection[288] are also applicable to LCAs.[289]

8. Certification-Related Functions of the Information Security Agency[290]

To better control LCAs and improve the reliability and security of digital signatures, the KISA is empowered with the following responsibilities:

- assist in the initial examination of the facilities and equipment held by an applicant for a LCA's license;[291]
- assist in the inspection of the LCA;[292]
- examine the LCA's security measures and give technical assistance as needed;[293]
- oversee regular inspections of the security of the LCA's facilities and equipment;[294]
- when necessary, issue and control certificates in lieu of the LCA;[295]
- develop technology pertaining to certification, dissemination, and standardization of digital signatures;[296]
- promote international cooperation on recognition of digital signatures and research and development of

287. *Id*. art. 24(1).

288. *Id*. art. 24(2). The confidentiality provisions are found in articles 22 through 32, 36(1), 54, 55, 62, 66, and 67 of the Act on Promotion of Information and Communications Network Utilization and Information Protection. *Id*. "The provider of information and communications service" is deemed a LCA and the user is deemed a subscriber. *Id.*

289. *Id*.

290. *Id.* art. 25.

291. *Id.* art. 25(1)(1); *see also id*. art. 4.

292. *Id.* art. 25(1)(2); *see also id*. art. 14(1).

293. *Id.* art. 25(1)(3); *see also id*. art. 18.3

294. *Id.* art. 25(1)(4); *see also id*. art. 19(2).

295. *Id.* art. 25(1)(5). For example, this might be necessary on a temporary basis when a LCA's license has been revoked. On an interim basis, the KISA might have to assume the LCA's duties. *See id*. art. 25(1)(5).

296. *Id.* art. 25(1)(6).

digital signature certification systems;[297] and
- perform other pertinent functions pertaining to digital signature certification.[298]

Whenever the KISA assumes duties that are normally carried out by the LCA, the KISA shall be governed by the DSA.[299] Furthermore, whenever the KISA assumes the LCA's duties (for example, "examination, technical assistance, inspection, issuance of authorized certificates"), the KISA may levy charges for the services it provides.[300]

9. Responsibilities of Relying Third Parties[301]

Relying third parties must carry out the following verification procedures to ensure the authenticity of a certified digital signature:[302]
- whether the certificate is still valid;[303]
- whether the certificate has been suspended or revoked;[304] and
- other matters as required by Articles 15(2)(7) and (8) of the DSA.[305]

When relying third parties verify a digital signature using a certificate, they cannot demand a specific LCA to issue the certificate. However, an exception does exist for a "justifiable reason."[306] The relying third party must ordinarily assume that the certificates issued by all LCAs are equally reliable and secure.

---

297. *Id.* art. 25(1)(7).

298. *Id.* art. 25(1)(8).

299. *Id*. art. 25(2). These are the specific provisions of the DSA which will become applicable to the KISA: articles 3, 6, 7, 15-18, 18-2, 18-3, 19(1), and 22. *Id*. art. 25(2). Using the DSA's terminology, the KISA will become the LCA and the no-longer-active LCA will become the subscriber. *Id*. art. 25(2).

300. *Id*. art. 25(3).

301. *Id*. art. 25-2.

302. *Id*. art. 25-2. Verification procedures are expressed in Articles 15(2)(1)–(6) of the DSA. *Id*. art. 25-2.

303. *Id*. art. 25-2(1).

304. *Id*. art. 25-2(2).

305. *Id*. art. 25-2(3).

306. *Id*. art. 25-3.

G. Governmental Adoption of Digital Signature Certification Policy[307]

1. General Policies

To promote the research and development of digital signatures and certification, their security and reliability, the government adopts the following policies:[308]

- security and reliability of digital signatures and the encouragement of their use;[309]
- cooperation among LCAs in the attainment of common standards for digital signatures and certificates and mutual recognition of certification activities;[310]
- promotion of research and development of digital signature techniques;[311]
- education and encouragement of the general public to use digital signatures;[312]
- continual improvement of digital signature and certification systems to encourage the wide use of digital signatures;[313]
- assistance and provision of pertinent information to organizations with connections to digital signatures;[314]
- protection of subscribers and relying third parties;[315]
- international cooperation through reciprocal recognition of foreign digital signatures and certificates;[316]
- promotion of the digital-signature-related industry and

307. *See id*. art. 26-2(6).

308. *Id*. art. 26-2.

309. *Id*. art. 26-2(1).

310. *Id*. art. 26-2(2).

311. *Id*. art. 26-2(3).

312. *Id*. art. 26-2(4).

313. *Id*. art. 26-2(5).

314. *Id*. art. 26-2(6).

315. *Id*. art. 26-2(7). The government establishes procedures to address complaints of subscribers and relying third parties against LCAs, and associated demands for reimbursement of damages. *Id*. art. 27(1). Such procedures are determined by the Ordinance of the MIC. *Id*. art. 27(2).

316. *Id*. art. 26-2(8).

the personnel needed by that industry;[317]
- the allocation of the LCA's security concerns;[318]
- adoption of "pilot projects" to promote the widespread use of digital signatures;[319]
- development and use of encryption techniques to achieve better reliability and security of electronic messages;[320] and
- other policies that may be necessary to achieve enhanced reliability, security, and use of digital signatures.[321]

2. Policies Toward International Convergence and Mutual Recognition

To achieve greater international reciprocal recognition of digital signatures, the MIC undertakes the following policies:
- research pertaining to international standards of reciprocal recognition of foreign-issued digital signatures and certificates;[322]
- establishment of internationally recognized standards of mutual recognition of foreign-issued digital signatures and certificates, and encouragement of a similar policy to be adopted by all countries of the world;[323]
- adjustments to the DSA, to bring it within the internationally recognized standards referenced in the preceding two policies;[324] and

317. *Id*. art. 26-2(9).

318. *Id*. art. 26-2(10).

319. *Id*. art. 26-2(11).

320. *Id*. art. 26-2(12).

321. *Id*. art. 26-2(13).

322. *Id*. art. 26-3(1)(1).

323. *Id*. art. 26-3(1)(2). Under Article 27 of the DSA, the government is authorized to enter into agreements with foreign governments for the reciprocal recognition of electronic signatures. *Id*. art. 27-2(1). Such agreements have the effect of giving foreign LCAs the same legal status as domestic LCAs, and also give foreign-issued certificates the same legal status as domestic-issued certificates. *Id*. art. 27-2(2). The agreements will be given a public notice by the MIC. *Id*. art. 27-2(3). Furthermore, such agreements result in foreign digital signatures and foreign certificates having the same legal effect as domestic ones. *Id*. art. 27-2(4).

324. *See id.* art. 26-3(1)(3).

- adoption of other policies pertaining to the adoption of the internationally recognized standards referenced in the preceding three policies.[325]

The MIC may enlist other agencies to assist in achieving internationally-recognized standards.[326] If it does so, the MIC may reimburse the other agencies for associated expenses.[327]

3. Policies Toward Research and Development (R & D) and Personnel Education

The MIC has the following policies regarding technical research and training:

- furtherance of R & D of digital signature techniques;[328]
- cooperation in disseminating and transfer of digital signature techniques;[329]
- provision of digital signature techniques and cooperating with, other relevant agencies and organizations;[330]
- promotion of the gathering of data pertaining to the supply and demand of personnel with digital signature-related expertise, and a concomitant policy of increasing the supply of manpower that is in demand but in short supply;[331] and
- other necessary policies affecting R & D and training of experts.[332]

4. Policies Regarding Implementation of Pilot Projects

The MIC establishes "pilot projects" designed to encourage greater use of digital signatures.[333] Specific details pertaining to

325. *Id.* art. 26-3(1)(4).

326. *Id.* art. 26-3(2).

327. *Id.* The Decree of the MIC provides the required conditions that must be present for reimbursement of other agencies' expenses to be allowed. *Id.*

328. *Id*. art. 26-4(1).

329. *Id.* art. 26-4(2).

330. *Id.* art. 26-4(3).

331. *See id.* art. 26-4(4).

332. *Id*. art. 26-4(5).

333. *Id*. art. 26-5(1).

these projects are stated in the Ordinance of the MIC.[334] The MIC also administers technical, administrative, and financial assistance for the benefits of these projects.[335]

5. *Policies Pertaining to Achievement of Greater Use of Digital Signatures*

The government adopts the following policies designed to increase usage of digital signatures:

- assistance to organizations and persons by central and local governments to encourage experimentation with digital signatures;[336]
- encouragement of more reliable and secure digital signatures by giving reduced fees if authorized digital signatures are used, that is, those verified by a certificate issued by a LCA;[337] and
- financial assistance to organizations executing a project related to digital signatures which is also designed to encourage greater use of them.[338]

H. Criminal Offenses and Penalties

1. Offenses Resulting in Maximum Penalty

The following offenses are punishable by imprisonment not to exceed three years or by a fine not to exceed 30 million won:[339]

- violation of Article 21(3) of the DSA by maintaining possession of a subscriber's private key without his permission, or using or disclosing the subscriber's private key without the subscriber's consent after receipt of the private key from the subscriber;[340]
- violation of Article 23(1) of the DSA by using another

334. *Id.*

335. *Id.* art. 26-5(2).

336. *Id.* art. 26-6(1).

337. *Id.* art. 26-6(2).

338. *See id*. art. 26-6(3).

339. *Id*. art. 31. As of the writing of this article, 30 million South Korean *won* was approximately U.S. $31,000. Currency Converter, *supra* note 223.

340. DSA, *supra* note 27, art. 31(1).

person's private key without his permission, or disclosing another person's private key;[341] and

- violation of Article 23(2) of the DSA by procuring the issuance of a certificate in the name of another person by pretending to be that person, or abetting such an issuance.[342]

2. Offenses Resulting in Moderate-Level Penalty[343]

The following offenses are punishable by imprisonment not to exceed one year or by a fine not to exceed 10 million won:[344] (1) violation of Article 22(2) of the DSA due to the LCA's failure to retain the subscriber's certificates,[345] and (2) violation of Article 25-3 due to a relying third party insisting that a digital signature be verified only by a certificate issued by a specifically named LCA.[346]

3. Aiding and Abetting Maximum or Moderate Level Offenses

If an agent, employee, or other representative of a person or corporation has aided or abetted in the commission of a maximum or moderate level offense, that party is punished by a fine as provided Article 31 or 32 of the DSA, respectively.[347]

4. Offenses Resulting in Lesser Penalty

The following negligent acts are punishable by a fine[348] not exceeding 5 million won:[349]

---

341. *Id*. art. 31(2).

342. *Id*. art. 31(3).

343. This section is an amendment to the original DSA and was added by Act No. 6585 on Dec. 31, 2001. *Id*. art. 31.

344. *Id*. art. 32. As of the writing of this article, 10 million South Korean *won* was approximately U.S. $10,300. Currency Converter, *supra* note 223.

345. DSA, *supra* note 27, art. 32(1).

346. *Id*. art. 32(2).

347. *Id*. art. 33.

348. *See* i*nfra* notes 363-366 and accompanying text (discussing the process for imposing fines).

349. DSA, *supra* note 27, art. 34(1). As of the writing of this article, five million South Korean *won* was approximately U.S. $5,200. *See* Currency Converter, *supra* note

- violation of Article 6(1) or 6(2) or the DSA[350] by failing to report the CPS or any modifications thereof to the MIC,[351] or violation of Article 6(3) of the DSA[352] by failing to implement the MIC's order to modify the CPS;[353]
- violation of Article 7 of the DSA[354] by refusing to provide LCA service without an excuse,[355] or for unlawful discrimination against classes of subscribers or relying third parties;[356]
- violation of Article 9(1) of the DSA by failing to file a report;[357]
- violation of Article 10(1) of the DSA by failing to inform subscribers or the MIC upon cessation of certification work, or violation of Article 10(2) of the DSA by the LCA's failing to inform subscribers or the MIC that it has gone out of business;[358]
- violation of Article 10(3) of the DSA by failing to transfer its certificates to another LCA when it is going out of business, or violation of Article 12(2) of the DSA by the LCA's failing to report the impossibility of such a transfer;[359]
- violation of Article 14(1) of the DSA by failing to submit relevant documents and materials to the MIC, or by submitting false documents and materials to the MIC, or by refusing to cooperate with the MIC by not allowing the MIC to enter its worksite for inspection;[360]

223.

350. These violations include cases of *mutatis mutandis* under Article 25(2) of the DSA.

351. *See* DSA, *supra* note 27, art. 34(1)(1) (instituting fines for violations of procedures mandated by Article 6 of the DSA); *see also id.* art. 6(1)-(2).

352. *See supra* notes 173, 174 and accompanying text.

353. *See* DSA, *supra* note 27, art. 34(1)(1) (instituting fines for violations of procedures mandated by Article 6 of the DSA).

354. *See supra* notes 176, 177 and accompanying text.

355. DSA, *supra* note 27, art. 34 (1)(2).

356. *Id.*

357. *Id.* art. 34(1)(3).

358. *Id.* art. 34(1)(4).

359. *Id.* art. 34(1)(5).

360. *Id.* art. 34(1)(6).

- violation of Article 21(4) of the DSA by failing to give a notification;[361] and
- violation of Article 23(3) of the DSA by using a similar mark to lead others to believe that an unauthorized certificate is an authorized one, or by falsely stating that a certificate is authorized.[362]

The fine is imposed and collected by the MIC.[363] During the first thirty days after it has been imposed, the fined party may file an objection with the MIC.[364] The MIC will then notify the court of competent jurisdiction, and the matter will proceed to trial under the Non-Contentious Case Litigation Procedure Act.[365] If the party does not timely pay the fine and does not file an objection within the time allotted, the government will collect the debt employing the same procedure as that used in reference to payment default on national taxes.[366]

VI. E-COMMERCE TRANSACTIONS CONSUMER PROTECTION ACT

A. Purpose, Overlaps with Other Acts, and Selected Basic Definitions

The purpose of the Act on the Consumer Protection in the Electronic Commerce Transactions[367] is to further the growth of e-commerce sales of goods and services by enhancing consumer confidence in the security and fairness of purchases.[368] If the CPA overlaps with other acts containing protections for cyber-buyers,[369] the CPA will take precedence over the others, with this proviso: if another act offers more protection for consumers

361. *Id.* art. 34(1)(7).

362. *Id.* art. 34(1)(8).

363. *Id.* art. 34(2).

364. *Id.* art. 34(3).

365. *Id.* art. 34(4).

366. *Id.* art. 34(5).

367. CPA, *supra* note 27.

368. *Id.* art. 1. If a consumer desires to bring a lawsuit against a seller based upon alleged violations of the CPA, the district court in the consumer's residence ordinarily has exclusive jurisdiction over the case, unless the consumer had no evident address at the time of filing the lawsuit. *Id.* art. 36.

369. *See e.g.* ECA, *supra* note 27, arts. 15–18.

than the CPA, it will be applied.[370] The Federal Trade Commission (FTC) is responsible for the implementation and administration of the CPA.[371] Business operators engaged in e-commerce are required to register with the FTC.[372] Implementation regulations have been promulgated by Presidential Decree (executive order) for the CPA, and they are contained in the Enforcement Decree of the Act on the Consumer Protection in the Electronic Commerce Transactions (Enforcement Decree or ED).[373]

Six basic definitions are included in the CPA:[374]

---

370. CPA, *supra* note 27, art. 4.

371. To achieve its functions, the FTC may delegate some of its authority to other agencies, the Mayor/*Do* governor, or to business firms. *(A "Do" is a Korean province.) Id.* art. 38 (amended by Act No. 7487 of Mar. 31, 2005, effective Apr. 1, 2006); *see* Presidential Decree, *supra* note 372, art. 40. Furthermore, several portions of the Monopoly Regulation and Fair Trade Act (MRFTA), 1980 Act No. 3320, amended 2002 (S. Korea), are applicable to some of the administrative duties of the FTC: (1) MRFTA art. 42–45 and 52 apply to the FTC deliberative decisions; (2) MRFTA art. 50(1)–(4) apply to the FTC's inspection procedure; (3) MRFTA art. 53, 53-2, 54, 55 and 55-2 apply to the filing of objections to the decisions of the FTC, their suspension of execution of orders of corrective measures, and exclusion jurisdiction pertaining to lawsuits; and (4) MRFTA art. 62 applies to the FTC commissioners as they carry out their duties. *See id.* art. 39.

372. CPA, *supra* note 27, art. 37(1). The application for registration must contain the following information relating to the business operator: (1) purpose; (2) title; (3) addresses of main office, branch offices, and website; (4) its representative's name, "resident registration number," telephone number and e-mail address; (5) date of incorporation or creation; (6) number of employees and branches; (7) manpower statement; (8) financial statement and degree of access to financial resources; and (9) important items of equipment. 13 STATUTES OF THE REPUBLIC OF KOREA (Korean Legislation Research Institute 2002) [hereinafter Presidential Decree]. The FTC must be informed within twenty days of any modifications to this information. *Id.* art. 39.

373. 13 STATUTES OF THE REPUBLIC OF KOREA 487 (Korean Legislation Research Institute 2002) [hereinafter Enforcement Decree] (enacted as Presidential Decree No. 17684, effective July 24, 2002; amended by Presidential Decree No. 18312, effective Mar. 17, 2004).

374. CPA, *supra* note 27, art. 2. The other three definitions are of: (1) "electronic commerce transaction"—the same definition expressed in Article 2(5) of the ECA is adopted by the CPA; (2) "consumer"—the user of products or services sold by "business operators for everyday consumption," but they must be end users (not users of raw materials, intermediate goods, or capital goods) *Id.* art. 2(5); *see also* Enforcement Decree, *supra* note 373, arts. 2(1)–(4) (including the following under the "consumer" rubric: business purchasers buying under the same terms as a consumer, multilevel salesmen, and small-scale farms and fisheries, respectively); and (3) "business

(1) "mail order" refers to the provision of information regarding the sale of goods and services by mail, telecommunications or other means, and to sell goods and services pursuant to an offer from a consumer;[375]

(2) "mail-order distributor" is one whose business is selling by mail order, or one who carries out mail order business under a contract with a mail-order distributor;[376] and

(3) a "mail order brokerage" carries out its sales using a cybermall, which is a website used to consummate transactions of contracts to buy and sell goods and services.[377]

B. Limitations and Precedence of the CPA

1. Limitations

The CPA's applicability has well-defined limitations.[378] The CPA does not apply when the buyer is making a purchase for a commercial reason.[379] In addition, the full-disclosure requirements[380] do not apply in the case of regular, recurring transactions that are uniform in nature.[381] These requirements also do not apply in the case of transactions relating to sales

operator"—a manufacturer, importer, or seller of goods and services. CPA, *supra* note 27, art. 2(6).

375. CPA, *supra* note 27, art 2(2). Note that telemarketing is excluded from this definition.

376. *Id.* art. 2(3).

377. *Id.* art. 2(4). Furthermore, all business firms engaged in e-commerce should register with the FTC. *Id.* art. 37.

378. *See id.* (amended by Act No. 7487, Mar. 31, 2005, effective Apr. 1, 2006).

379. *Id.* art. 3(1). In other words, the CPA only applies to those making purchases for consumer goods and services, not business goods and services. However, multilevel salespersons under Article 2(6) of the Door-to-Door Sales Act are excluded from this restriction. *Id*.

380. These requirements are covered in Article 13(2) of the CPA (disclosure of all pertinent facts in a document is required by the seller before the sales contract is consummated), and Article 16(1) of the CPA (disclosure of all pertinent facts, including the cost of the goods/services and other expenses incurred by the buyer, must be included in a document delivered to the buyer with the goods).

381. *Id.* art. 3(2)(1). This provision also excludes those transactions enumerated under the "Ordinance of the Prime Minister." *Id.*

that employ different means of distribution covered by other laws. This does not include transactions governed by the civil law or the Door-to-Door Sales Act.[382] Mail-order brokers serving as middlemen between two parties, neither of which is a mail-order distributor, also will not be subject to Articles 13–19 of the CPA,[383] Finally, some other transactions are exempt from Articles 12–20 of the CPA.[384]

2. General Precedence

Notwithstanding the above limitations, the CPA takes precedence over other statutes containing consumer protections in e-commerce provided the CPA is in agreement with those statutes.[385] The only exception to the CPA's precedence is when another statute in question provides more rights and protections for consumers, in which case the other statute controls.[386]

C. E-Commerce Transactions

1. Employment of Electronic Documents

If the seller agrees to use electronic documents but does not send those documents to the buyer's designated address,[387] the seller cannot claim that the buyer received the documents. This scenario will be the case, notwithstanding the provisions of Article 6(2)(2) of the ECA.[388] However, there are three

382. *Id.* art. 3(2)(2).

383. *Id.* art. 3(3).

384. *Id.* art. 3(4). These transactions include (1) security firms' transactions carried out under Article 2(9) of the Securities and Exchange Act; (2) financial firms' transactions pertaining to sale of financial products enumerated in the Presidential Decree (Article 3 of the PD defines them as those which are carried out by the financial institutions affected by Articles 38(1)–(12) of the Act on the Establishment of Financial Supervisory Organizations, financial organizations created by other Acts, or those established under the authority of the central administrative agencies); and (3) transactions to sell food and commodities to a local buyer. *Id.*

385. CPA, *supra* note 27, art. 4.

386. *Id*.

387. The address referenced in ECA art. 2(2).

388. As previously discussed, Article 6(2)(2) of the ECA provides that when the receiver has not designated a computer information system where the message is to be sent, the deemed time of receipt is when the message enters a system that is managed by

exceptions:

(1) there is an urgent need for the document;[389]

(2) the buyer believes that digital documents will be used to consummate the transaction;[390] or

(3) the customer converts[391] the digital form to hard copy.[392]

If the seller desires to send an electronic document with a digital signature[393] affixed, he must inform the buyer of the procedure to be used for validation and acceptance of the signature.[394] However, the seller should respect the principles of technological neutrality and must not try to explicitly compel the buyer to use a specific type of digital signature, or require such high standards that only one particular type or class of digital signatures qualifies.[395]

2. Recording the Electronic Transaction

The seller should retain transaction records at its website and make it easy for buyers to access those records.[396] This

---

the receiver. ECA, *supra* note 27.

389. There must be an urgent need to make contact and E-mail must be the only means of communication available. Presidential Decree, *supra* note 372, art. 4(4).

390. The consumer must not deny the validity of the electronic message, and it is not detrimental to the consumer's interest. *Id.* art. 4(3).

391. The consumer has already printed out the electronic message. *Id.* art. 4(2).

392. CPA, *supra* note 27, art. 5(1).

393. *See* DSA, *supra* note 27, art. 2(2).

394. CPA, *supra* note 27, art. 5(2). In the main body of the e-mail containing the message and the digital signature, the business operator should inform the buyer that (1) the message with the digital signature affixed is valid; and (2) the method needed to be used to "output an electronic document with a digital signature." Presidential Decree, *supra* note 372, art. 5.

395. CPA, *supra* note 27, art. 5(3).

396. *Id.* art. 6(1). The "object, extent and period of transaction" of records required to be kept, archival methods, and methods of access are determined by Presidential Decree. *Id.* art. 6(3). The following retention periods are applicable to mail-order brokers: (1) advertisement and indication records—six months; (2) contract and cancellation records—five years; (3) supply of goods, and payment records—five years; and (4) customer complaints and records of customer disputes—three years. Presidential Decree, *supra* note 372, art. 6(1). To satisfy the requirement allowing consumers to peruse records, the business operator is obliged to maintain records at its website and to give access of the consumer to them. *Id.* Additionally, the business operator must comply with a consumer request and allow the consumer to peruse and photocopy relevant documents

transaction information, along with some identification data of the consumer,[397] should be archived notwithstanding Article 30(3) of the Act on Promotion of Utilization of Information & Communications Network. The requirement holds true even if the buyer decides to withdraw his permission for the seller to use his private information.[398]

3. Confirmation of Terms

The seller is responsible for establishing reliable confirmation methods to minimize misunderstandings in e-commerce. The seller is also responsible for establishing easy-to-use methods for the buyer to change terms before finalizing the transactions.[399]

4. Electronic Payments: Security Procedure

In the consummation of an e-commerce transaction with electronic payment, the seller and the payment service provider (e-settlor)[400] must ensure that security of pertinent information is maintained at all times.[401] Both the seller and the e-settlor must scrutinize information inserted by the buyer to determine whether it reflects the intentions of the buyer.[402] The seller and the e-settlor should send electronic invoices to the buyer.[403] Once the payment is finished, the seller should provide easy access of

---

at its business premises. *Id.* art. 6(2).

397. Ordinarily, identification data is limited to the buyer's name, address, and ID number. CPA, *supra* note 27, art. 6(2).

398. *Id.* art. 6(2).

399. *Id.* art. 7.

400. E-settlors include "the issuer of the electronic settlement means concerned, provider of electronic settlement service, or persons who aid or intermediate the execution of electronic settlement service," and fall into one of the following categories: (1) financial institutions; (2) credit card business operators; (3) issuers of the settlement means that stores monetary value electronically, and is payable at time of purchase of the goods; (4) a business providing a settlement service via wire or wireless terminals; (5) information communications service providers; and (6) an agency or brokerage service of electronic settlement. Presidential Decree, *supra* note 372, art. 8.

401. CPA, *supra* note 27, art. 8(1).

402. *Id.* art. 8(2).

403. *Id.* art. 8(3).

the payment information to the buyer at any time.[404] To keep the buyer well informed in cybermall transactions, the e-settlor should point out information relating to the payment method, restriction in usage of the item purchased, and consumer protections given to the buyer.[405] If there is a payment dispute between the buyer and seller, the e-settlor should intervene and provide the parties with information relating to the payment.[406]

5. Delivery Firms' Duty to Cooperate in Dispute Settlement

A firm that has the duty is to deliver goods purchased in e-commerce should cooperate with the buyer and seller whenever they have a dispute pertaining to damages of goods in transit.[407]

6. Management of the Mail-Order Broker's Website

In order for the consumer to easily identify the mail order broker at its website, the following information must be clearly displayed:

- trade name and name of director;
- business address, including the consumer complaint handling location;
- telephone number and e-mail address;
- business license number;
- terms and conditions expected to be complied with by the buyer in doing business at the website; and
- other consumer protections specified in the Presidential

404. *Id.* For the convenience of both the seller and the buyer, this information is often provided at the seller's website.

405. *Id.* art. 8(4). The settlement means must be used in not less than three cybermalls. Presidential Decree, *supra* note 372, art. 9.

406. CPA, *supra* note 27,. art. 8(5). Specifically, the e-settlor should provide access to documents pertaining to the customer's payment and to documents relating to the seller's confidentiality procedures that are pertinent to the transaction in question. Presidential Decree, *supra* note 372, art. 10.

407. CPA, *supra* note 27, art. 9. This also applies when the delivery is carried out by a "communication network" under Article 2(1) of the Act on Promotion of Information and Communications Network Utilization and Information Protection. *Id*. The party delivering the goods should provide access to the delivery records and to records pertaining to an accident or other cause of the delay. Presidential Decree, *supra* note 372, art. 11.

Decree.[408]

If operations of the website violate the CPA, the manager of the website must be willing to take corrective measures to eliminate the violations.[409]

7. Duty of Confidentiality

The business operator has a duty to maintain confidentiality of buyer-related information. At all times, the seller must use the information fairly, commensurate with the requirements of the Act on Promotion of Information and Communications Network Utilization and Information Protection.[410] Pursuant to the Presidential Decree, the business operator should take measures to confirm the identity of the party with whom transactions are being conducted. [411] If damages occur or are anticipated due to breach of confidentiality, the damage should be rectified.[412]

8. Mail-Order Distributor's Obligation

The seller must provide the following information either to the FTC, the mayor of the city where business is being conducted, or the provincial governor:

- trade name, address, and telephone number;
- if a corporation, the name and ID number of the representing director;
- the e-mail address and website address; and
- other identification information as determined by the Presidential Decree.[413]

---

408. *Id.* art. 10(1) (amended by Act No. 7487, Mar. 31, 2005, effective Apr. 1, 2006).

409. *Id.* art. 10(2).

410. *Id.* art. 11(1).

411. Specifically, the consumer should be informed of any unauthorized use of his confidential information, his records should be restored to their original state, and if applicable, the consumer's damage should be restored to make the injured party whole. Presidential Decree, *supra* note 372, art. 12.

412. *Id.* art. 11(2).

413. *Id.* art. 12(1). Furthermore, a certified copy of the corporate registration and a copy of the business registration should be filed. Presidential Decree, *supra* note 372, art. 13. This information-provision requirement does not apply to small-scale sellers and others exempted by the Presidential Decree. CPA, *supra* note 27, art. 12(1). The PD

If the seller wants to suspend, terminate, or resume operations of the business, this information must also be conveyed to the FTC, mayor, or governor.[414] The FTC's authority to post the seller-related information will be determined by the Presidential Decree.[415]

9. Mail-Order Distributor's Duty to Provide Information Relating to Transactions

When the mail-order distributor advertises goods and services, it must include this information:

- trade name;
- name of director;
- mailing address, e-mail address, and telephone number; and
- notification number of the report submitted to the FTC under Article 12 of the CPA.[416]

To ensure the buyer's understanding before the contract between the parties is consummated, the mail-order distributor should supply a document to the buyer containing the following information:

- a list of the sellers and suppliers of the goods;

---

exempts firms qualifying for a simplified version of the Value-Added Tax Act. Presidential Decree, *supra* note 372, art. 14(1). This exemption to the duty to report should be noted in any advertisements for mail order business. *Id.* art. 14(2). Any posting of information updates should be carried out under the directives in the Presidential Decree. CPA, *supra* note 27, art. 12(2). Within fifteen days after the modification is made, the pertinent modification documents should be filed with the FTC or the Mayor/*Do* governor, whereupon the modifications will be confirmed. Presidential Decree, *supra* note 372, art. 16. If the reports mentioned in Article 12 of the CPA are filed electronically, this should be performed with a data processing system that has been approved by the FTC and is commensurate with it. *Id.* art. 18(1).

414. CPA, *supra* note 27, art. 12(3). If the business has already closed, it should file the former certificate of report. Presidential Decree, *supra* note 372, art. 17. In communiques pertinent to these issues, the business operator must disclose its name and resident registration number. *Id.* art. 15.

415. CPA, *supra* note 27, art. 12(4). If the FTC posts information regarding mail-order distributors, it will inform the distributor in advance and give it an opportunity to correct any mistakes in the information before it is publicized. Presidential Decree, *supra* note 372, art. 19.

416. CPA, *supra* note 27, art. 13(1) (amended by Act No. 7487 of Mar. 31, 2005, effective Apr. 1, 2006).

- the name, kind, and content of goods;
- the price (or methods of determining the price), payment methods, and payment period;
- the time and method for delivery;
- the period in which the offer may be withdrawn, how to withdraw the offer, effects of withdrawal of the offer, and cancellation of contract;
- the warranty, refund and exchange policies, and the duration of each;
- the technical information relating to the sending and the installation of goods relating to digital media;
- the consumer complaint policies and procedure for attaining compensation for damaged goods;
- the terms and conditions of the transaction;
- information regarding the consumer's option to utilize an escrow system in payment, or to be protected with consumer damage compensation insurance; and
- other items prescribed in the Presidential Decree,[417] that is, other critical contractual terms besides price that may affect the consumer's decision to consummate the transaction, or other matters relevant to the consumer's attainment of compensation from the seller for his damages.[418]

10. Confirmation, Adjustment, and Shipment of Goods

A mail-order distributor has a duty to promptly confirm the receipt of an offer from a buyer and to inform the buyer whether

417. *Id.* art. 13(2). Other examples of information that may be included are the sale date, geographical location of the sale, quantity of the sale, and geographical location of delivery. Presidential Decree, *supra* note 372, art. 20(2).

418. CPA, *supra* note 27, art. 13(2) (amended by Act No. 7487 of Mar. 31, 2005, effective Apr. 1, 2006). Obviously, the seller is required to "execute faithfully" the agreement that has been entered into with the buyer. *Id.* art. 13(5). The FTC will formulate rules regarding the announcement of the identification of the seller. *Id.* art. 13(3). The characteristics of the announcement may be varied according to the type of transaction or the category of goods. *Id.* When transacting with a minor, the minor should be informed that if his legal representative does not affirm the contract, it may be cancelled by either the minor or the legal representative. *Id.* This is a new amendment added by Act No. 7487 of Mar. 31, 2005; effective Apr. 1, 2006.

the item is available for sale.[419] The mail-order distributor should also have an established procedure for the buyer to adjust the terms of sale before the contract he consummates the contract.[420]

Ordinarily, the mail-order distributor should ship the goods within seven days after the order is received.[421] However, if either full or partial advance payment is received,[422] the goods should be shipped within three days after the order is received.[423] If the parties have entered into an agreement concerning when the goods will be shipped, the agreement controls.[424]

If unforeseen difficulties arise in shipment of the goods, the buyer should be informed of the reasons for the delay.[425] However, if unforeseen difficulties arise in either a full or partial prepaid situation, action to refund the money to the buyer should be commenced within three days after receipt of the payment.[426]

If the goods are shipped as promised, the mail-order distributor should keep the buyer informed of facts pertaining to delivery of the goods. [427] The FTC has the responsibility of establishing the measures to be taken in this regard, and the distributor shall follow the FTC's measures.[428]

11. Consumer's Withdrawal from the Agreement

When entering into a contract for an online purchase, the buyer is given a window of opportunity to withdraw from the agreement, as follows: (1) seven days from the date of receipt of

419. *Id.* art. 14(1).

420. *Id.* art. 14(2).

421. *Id.* art . 15(1).

422. The CPA refers to this as "prepaid mail order." *See id*

423. *Id.* (amended by Act No. 7487 of Mar. 31, 2005, effective Apr. 1, 2006).

424. *Id*.

425. *Id.* art. 15(2) (amended by Act No. 7487 of Mar. 31, 2005, effective Apr. 1, 2006).

426. *Id.* Articles 18(1) and 18(5) are applied *mutatis mutandis* if a refund is due. *Id.* art. 15(4).

427. *Id.* art. 15(3).

428. *Id.*

the written document[429] containing the terms of the contract,[430] but if the stock of goods runs out, the operative counting date of the seven days is when the stock is replenished or the replenishment is launched;[431] or (2) if the buyer does not receive a written document,[432] or the document does not contain the address of the mail-order distributor, or if the buyer cannot timely withdraw her offer due to lack of knowledge of the mail-order distributor's new address, then the seven-day period begins to run at the time the buyer knows, or has the ability to learn, the new address.[433]

However, the buyer is ordinarily not allowed to withdraw from the agreement in the following situations:

(1) the goods have been damaged or destroyed due to the buyer's acts;[434]
(2) the value of the goods has been substantially reduced due to the buyer's acts;[435]
(3) the value of the goods has been so reduced that resale of them has become difficult or impossible;[436]
(4) the package has been destroyed;[437] or
(5) other situations determined in the Presidential Decree.[438]

---

429. *See id.* art. 13(2).

430. *Id.* art. 17(1)(1). Additionally, any contract in violation of Articles 17–19 of the CPA and disadvantageous to consumers is automatically invalid. *Id.* art. 35.

431. *Id.* art. 17(1)(1).

432. *See id.* art. 13(2).

433. *Id.* art. 17(1)(2).

434. *Id.* art. 17(2)(1). However, it is not considered negligence to have merely opened the package to confirm the contents of the shipment. *Id*.

435. *Id.* art. 17(2)(2). Goods falling in this category should be so indicated by the seller on the package to give notice to the buyer. *Id.* art. 17(6). Furthermore, the consumer should be liberally allowed to withdraw in a situation involving pilot products. *Id*.

436. *Id.* art. 17(2)(3).

437. *Id.* art. 17(2)(4).

438. *Id.* art. 17(2)(5). Generally, the consumer is not allowed to cancel the order whenever that would result in unrecoverable loss to the seller. An example is where the seller produced goods on special order that are tailor-made for the consumer; such goods are not easily sold to others. The buyer must have been made aware of the potential unrecoverable loss of seller and nevertheless agreed to the special order. Presidential Decree, *supra* note 372, art. 21.

Notwithstanding the applicability of one of the previously mentioned situations, if the mail-order distributor does not pursue the measures under Article 17(6) of the CPA, the consumer may cancel the contract.

Notwithstanding the two previous paragraphs, if the contents of the shipment are different from the advertisement and from the label, or the contract has been performed in a manner different from what the parties agreed upon, the window of opportunity for the consumer to withdraw from the agreement becomes substantially longer. For example, this window will be three months from the date of receipt of the goods, or thirty days from the time he either knew, or should have known, of the nonconformity of the shipment with the order, or of the nonconformity of the performance.[439]

If it becomes difficult to cancel the order due to the presence of factors (2), (3), (4) or (5) listed above, the mail-order distributor should

(1) indicate that fact on the package of the goods or in another prominent location where it will be easily noticed by the buyer;
(2) supply test goods; or
(3) take whatever action is necessary to facilitate the buyer's ability to cancel the order.[440]

If the withdrawal[441] is carried out by a written document, the withdrawal becomes effective the day it is sent.[442] If the mail-order distributor contests the buyer's right of withdrawal and contends the buyer has misstated the facts, that is, whether the contract was signed, or whether or when the goods were supplied, the burden falls to the mail-order distributor to offer proof regarding his version of the facts.[443]

---

439. CPA, *supra* note 27, art. 17(3).

440. *Id.* art. 17(6) (amended by Act No. 7487 of Mar. 31, 2005, effective Apr. 1, 2006).

441. *See id.* arts. 17(1) or (3).

442. *Id.* art. 17(4).

443. *Id.* art. 17(5) (amended by Act No. 7487 of Mar. 31, 2005, effective Apr. 1, 2006).

12. Consumer's Withdrawal from the Agreement: Aftermath

If the buyer withdraws from the agreement,[444] he must return the goods to the seller.[445] If payment has already been made to the seller, the mail-order distributor must reimburse the buyer within three days after the goods have been returned.[446] If reimbursement is not made within three days, interest payable to the consumer will begin to accrue on the fourth day.[447] If the buyer has prepaid with a credit card, and has later withdrawn from the agreement, the mail-order distributor should reimburse the credit card company and ask it to cancel its demand for payment from the consumer.[448] A credit card company that has been paid by the mail-order distributor should promptly give a refund to the buyer, or credit his account.[449] If the credit card company delays in crediting the buyer's account, the mail-order distributor is responsible for paying interest to the buyer.[450]

Ordinarily, the mail-order distributor whose goods have been returned is still entitled to compensation for the benefits received by the consumer and the value of the goods.[451]

---

444. *See id.* arts. 17(1) or (3) (providing for such a withdrawal).

445. *Id.* art. 18(1).

446. *Id.* art. 18(2).

447. *Id.* The interest is required according to an announcement of the FTC. *Id.*

448. *Id.* art. 18(3). If the seller unjustifiably fails to reimburse the credit card company, the consumer should ask the credit card company "to offset the amount to be refunded by other debt the credit card company owes to the mail-order distributor" *Id.* art. 18(6). The consumer must provide documentary evidence to the credit card company showing the refund amount due and that cancellation occurred during the allowable period. If offset occurs, the credit card company should inform the mail-order distributor. Presidential Decree, *supra* note 372, art. 23. However, if the credit card company refuses to do this, and the buyer reacts by not paying the credit card company, the credit card company (and the mail-order distributor) should not try to blacklist the buyer by submitting negative information about her to a credit rating company. CPA, *supra* note 27, art. 18(7) (amended by Act No. 7487 of Mar. 31, 2005, effective Apr. 1, 2006). Article 22 of the PD elaborates on the meaning of "other means of settlement." *See* Presidential Decree, *supra* note 372, art. 22.

449. CPA, *supra* note 27, art. 18(4).

450. *Id.* art. 18(5). All parties in the chain connecting the seller to the buyer, that is, middlemen, e-settlors and others, have a duty to promptly take responsibility to ensure that the buyer is reimbursed as soon as possible. *Id.* art. 18(11).

451. *Id.* art. 18(8). Expenses that may be assessed against the consumer for his

Furthermore, the party returning the goods is responsible for expenses incurred in effecting the return.[452] In the extraordinary situation where there has been misleading advertisement or labeling, the mail-order distributor is regarded as the party at fault and bears responsibility for payment of expenses incurred in the return of the goods.[453]

13. Limitations on Damages

If a buyer withdraws from the contract due to his own fault, the seller will include the premium payment required when a payment is overdue.[454] Additionally, if the goods are returned, the seller shall be paid the larger of: (1) the usual rental fee of the goods, or the value of the benefit obtained from the use of the goods, or (2) the difference between the selling price of the goods and their value at the time they were returned.[455] Alternatively, if the goods are not returned, the buyer is liable for the selling price of the goods.[456] The FTC sets the applicable standards in computing damages.[457]

14. Responsibilities of Mail-Order Brokers

If an e-commerce buyer deals with a mail-order broker (MOB), and the MOB does not disavow responsibility for the damages to the goods in transit, then both the MOB and the party supplying the goods shall be jointly and severally liable for any damages to the goods in transit.[458] If the MOB is also a mail-order distributor,[459] the MOB carries duties and responsibilities

---

partial consumption include additional marketing expenses due to difficulty of re-sale of the un-consumed portion, a decrease in selling price due to the missing portion, or expenses of replacement of the consumed portion in a case of only the whole amount being salable in a situation of each unit having "identical divisible parts." Presidential Decree, *supra* note 372, art. 24.

452. CPA, *supra* note 27, art. 18(9). However, the seller is not entitled to damages incurred as a result of the buyer's withdrawal from the agreement. *Id.*

453. *Id.* art. 18(10); *see also id.* art. 17(3).

454. *Id.* art. 19(1).

455. *Id.* art. 19(1)(1).

456. *Id.* art. 19(1)(2).

457. *Id.* art. 19(2).

458. *Id.* art. 20(1).

459. *See id.* arts. 12–18.

because of that status,[460] with the following proviso: if the mail-order brokerage engages in acts at the request of the mail-order distributor, the mail-order distributor will be responsible for any promises made to the buyer that it would be responsible for as the MOB.[461]

The e-commerce seller who uses a MOB as a middleman remains responsible for "deliberate or accidental damage" of the goods during transit,[462] with the exception that the seller shall not be responsible if he has given "considerable attention"[463] to the matter in an attempt to prevent the occurrence of damage.[464]

The MOB should allow the consumer to access its website and identify information pertaining to the business operator offering the product or service.[465] If the MOB is an individual person and not a business operator, the MOB should provide the person's address and telephone number.[466]

15. Prohibited Acts

E-commerce sellers and mail-order distributors are forbidden from commission of the following acts:[467]

- lying, exaggerating, using deception or unfair methods of interference with the cancellation of an order or a contract;
- changing a business address or telephone number, or the address of a business website, to hamper cancellation of an order or contract;
- refusing to establish a customer complaint department, or assignment of inadequate staff or other resources to that department;
- sending goods before an order is received and then billing

460. *Id.* art. 20(2).

461. *Id.*

462. *Id.* art. 20(3).

463. *Id.* This seems to be about the same as "reasonable care" in U.S. law.

464. *Id.*

465. *Id.* art 20(4).

466. *Id.* The PD also suggests that the person's name be provided. Presidential Decree, *supra* note 372, art. 25(1).

467. CPA, *supra* note 27, art. 21 (amended by Act No. 7487 of Mar. 31, 2005, effective Apr. 1, 2006).

the customer, or billing a potential customer for no reason;

- attempting to compel a customer to accept a good or service via a communiqué by telephone, fax, or e-mail, despite the fact that the customer never expressed a desire to purchase the good or service; and
- using personal information of a person without consent or beyond the range of the consent given.[468]

Furthermore, the FTC may draft additional business standards to be observed by e-commerce sellers and mail-order distributors.[469]

16. Responsibilities of Mail Order Distributors Going Out of Business

Mail order distributors that are preparing to go out of business must cancel all contracts they have previously agreed to handle and must refund all prepaid remittances received from buyers. [470] These responsibilities also apply if the mail-order distributor has temporarily suspended its business, or has already closed its business.[471]

---

468. *Id.* art. 21(1). However, the last prohibition does not apply to the following acts: (1) where personal information must be used to deliver the goods; (2) where use of personal information is necessary to settle accounts after the goods are delivered; (3) where personal information is necessary to confirm the identity of the buyer; and (4) when other Acts create a situation in which personal information must be used. *Id.* art. 21(1)(6). Article 27 of the PD provides specific examples of situations in which a consumer's personal information must be used to prevent its "surreptitious use." It is also acceptable to provide the personal information to those who will be installing the goods or will provide service-after-the-sale. Presidential Decree, *supra* note 372, art. 26(2).

469. CPA, *supra* note 27, art. 21(2).

470. *See id.* arts. 17(1) and (3); *see also id.* 18(1)–(5).

471. *Id.* art. 22(1). If the mail-order distributor is unable to continue in business due to a legal bankrupt status, "the Fair Trade Commission or the Mayor/*Do* governor who has been reported under the provisions of Article 12(1) may delete the reported matters *ex officio*." *Id.* art. 22(2).

D. Protection of Consumers' Rights and Interests

1. Consumer Protection Guidelines

The FTC can promulgate consumer protection guidelines that will affect e-commerce business firms in the contracts they make with their customers.[472] Whenever a business firm makes contractual provisions that carry a lesser degree of protection for the consumer, the business firm should inform the consumer.[473]

2. Consumer Damage Insurance

The FTC strongly encourages e-commerce business firms and mail-order distributors to carry insurance[474] protection for the consumers they serve,[475] with the proviso that in the case of cybermall websites (refer to Article 8(4) of the CPA), the issuer of a settlement would be encouraged to do one of the following:

- carry a consumer-protection insurance policy under the Insurance Business Act;
- enter into a "contract of guarantee for payment against debt" under the Act on the Establishment of Financial Supervisory Organizations to provide for payment of

---

472. *Id.* art. 23(1).

473. *Id.* art. 23(2).

474. Article 28 of the PD contains two pages of meticulous legal requirements that must be complied with in a contract of consumer damage compensation insurance. *See* Presidential Decree, *supra* note 372, art. 28.

475. CPA, *supra* note 27, art. 24(1). However, in the case of a prepaid mail order, the customer may have the option of using an escrow system under Article 13(2)(1) of the CPA for protection, or he may require the mail-order distributor to provide insurance coverage. *Id.* art. 24(2) (added by Act No. 7487 of Mar. 31, 2005; effective Apr. 1, 2006). However, this option is inapplicable in the following situations: (1) the price of the goods is less than 100,000 *won*; (2) the payment is made by a credit card under Article (2)(3) of the Specialized Credit Financial Business Act; (3) the purchase is for goods sent through information and communications networks, or the forwarding of said goods cannot be confirmed by third parties as are referenced in Article 13(2)(10) of the CPA; (4) the goods are to be paid for in installments; and (5) other transactions which, in the opinion of the FTC, do not require the utilization of an escrow or insurance because these transactions are otherwise secured by another Act or because there are conditions similar to those described in items (1)–(4) immediately above. *Id.* art. 24(3) (added by Act No. 7487 of Mar. 31, 2005; effective Apr. 1, 2006). Details pertaining to the escrow system or insurance coverage referenced in Article 24(2) of the CPA will be provided in a PD. *Id.* art. 24(4) (added by Act No. 7487 of Mar. 31, 2005, becoming effective Apr. 1, 2006).

consumer damages; or

- enter into "mutual aid contract" with a mutual aid association under Article 24(1) of the CPA.[476]

A specific figure cannot be placed on the amount of insurance coverage that should be purchased. The coverage should be high enough to compensate consumers for the amount of their actual damages. Alternatively, the coverage should be great enough to satisfy the "issuer of settlement means."[477] Whoever is liable to pay the "consumer damage compensation" according to the insurance contract must pay it in a timely manner; otherwise, that party will be responsible for paying any late fees that are assessed.[478]

The party entering into an insurance contract should ensure that he does not submit an erroneous figure for the total sales amount.[479]

If a party in e-commerce carries consumer protection insurance, that party may use a marker of some sort to indicate that the party carries insurance coverage.[480] However, if a party has no insurance, it may not use a marker that erroneously indicates that the party has coverage.[481]

As an alternative to entering into an insurance contract, the sellers or the mail-order distributors are free to establish a mutual aid association for the purpose of protection of the consumer.[482]

---

476. *Id.* art. 24(1) (amended by Act No. 7487 of Mar. 31, 2005, effective Apr. 1, 2006).

477. *Id.* art. 24(5); *see also id.* art. 8(4).

478. *Id.* art. 24(6).

479. *Id.* art. 24(7).

480. *Id.* art. 24(8).

481. *Id.* art. 24(8). This is applicable *mutatis mutandis* to the escrow system referenced in Article 24(2) of the CPA. *Id.* art. 24(9).

482. *Id.* art. 24(10). Establishment of a mutual aid association is also referenced in Article 24(1)(3) of the CPA. The procedure to be used in the establishment of the mutual aid association would be the same as that found in the Article 35 of the Door-to-Door Sales Act, that will apply *mutatis mutandis*, but some of the wording has changed to reflect that it is now applicable to the CPA. *Id.* art. 24(10).

3. "Spam" Refusal[483]

The FTC is authorized to maintain a list of those who refuse to accept unsolicited "spam" messages by e-mail, fax, or telephone.[484] Before sending unsolicited messages, mail-order distributors should check the FTC's list to ensure that the message recipients are not on the list. It is not necessary to do this if the persons have already given their consent to mail-order distributors to send the messages.[485]

E. Inspection and Supervision

Anyone may report suspected violations of the CPA to either the FTC or the Mayor/Do governor.[486] However, if the alleged violations are more than five years old, neither penalties nor correctional measures shall be ordered by the FTC.[487] In no way does this excuse a party from abiding by an agreement entered into with a dispute arbitration organization under Article 33(1) of the CPA.[488]

If the parties believe that the CPA has been violated, the FTC or the Mayor/Do governor may carry out inspections of the suspected party or parties on an ex officio basis.[489] If the Mayor/Do governor is to execute the inspections, he must inform the FTC in advance. If both the FTC and the Mayor/Do governor plan to inspect, the Mayor/Do governor should defer to the FTC to handle inspections.[490]

---

483. *Id.* art. 24-2.

484. *Id.* art. 24-2(1). The FTC may delegate the maintenance of the anti-spam list to an organization within one of the following categories: (1) the consumers' organization established under the CPA; or (2) the e-commerce sellers' organization established under Article 27 of the CPA. *Id.* art. 24-2(3). The selection procedures will be announced by Presidential Decree. *Id.* art. 24(4). The FTC may partially or fully subsidize this organization for expenses incurred that pertain to this endeavor. *Id.* art. 25.

485. *Id.* art. 24-2(2).

486. *Id.* art. 26(4).

487. *Id.* art. 26(5).

488. *Id.* art. 26(5); *see also id.* arts. 32, 34 (discussing penalties and correctional measures).

489. *See id.* art. 26(1).

490. *Id.* art. 26(2). In cases of overlapping jurisdiction between the FTC and the Mayor/*Do* governor, the Mayor/*Do* governor "shall . . . suspend the investigation" unless there is a persuasive reason not to do so. *Id.*

After the inspection, the inspector should inform the inspected party of the results. If a written disposition was prepared, the inspected party should receive a copy of it.[491] If the CPA was violated, the FTC should order the violator to make a correction under Article 31, or to carry out "corrective measures" under Article 32. However, if the Mayor/Do governor carries out the inspection and believes that action is necessary under Articles 31 or 32, the Mayor/Do governor must first inform the FTC.[492] The FTC has a duty of oversight over the Mayor/Do governor. Accordingly, the FTC may want to confirm the Mayor/Do's findings by conducting its own inspection, or may ask the Mayor/Do governor to submit related documents that substantiate its findings.[493] The Mayor/Do governor should comply with the FTC's requests unless a special reason would compel otherwise.[494]

The FTC is authorized to search public databases for information about e-commerce sellers and mail-order distributors, including information on their violations of the CPA and other consumer protection laws,[495] and to distribute the information to consumers.[496] These parties may not object to the FTC's authorized search.[497] Furthermore, e-commerce sellers and mail-order distributors have a duty to provide information about themselves to the FTC and to the general public, and also to allow the FTC to distribute the information to consumers. [498] When the FTC requests information from the parties,[499] they

---

491. *Id.* art. 26(3).

492. *Id.* art. 30(1). The report may be in electronic form. Presidential Decree *supra* note 372, art. 32.

493. CPA, *supra* note 27, art. 30(2).

494. *Id*.

495. *See id.* art. 27(1).

496. *Id.* art. 28. Before publicizing the irregularities, the FTC should inform the business operator beforehand to give it an opportunity to explain and eliminate any misunderstanding that may exist. Presidential Decree, *supra* note 372, art. 30.

497. CPA, *supra* note 27, art. 27(2).

498. *See id.* art. 27(3).

499. The request should indicate to the business operator the information's purpose and use, the extent to which the information should be submitted, and the extent to which it will be shared. Presidential Decree, *supra* note 372, art. 29(1). The FTC is forbidden to use the information for any purpose other than that disclosed to the

may not refuse to divulge the information without good cause.[500]

However, the FTC must be fair in its evaluation of the e-commerce sellers and mail-order distributors.[501] Its standards and methods must be a matter of public record, and the standards must be applied impartially.[502] The FTC may require the evaluators to prepare reports containing operations data.[503] The goal of the evaluation is to obtain reliable and accurate information relating to the business firms' behavior toward protection of the consumer.[504]

F. Corrections and Penal Surcharges

1. Opportunity to Voluntarily Correct Before Sanctions are Imposed

If an e-commerce business is in violation of the CPA, it will be given an opportunity to rectify its behavior before sanctions are imposed.[505] The corrective plan will be drafted and presented to the culprit business for its consideration.[506] The business will then have ten days to decide whether it will accept the corrective agreement voluntarily.[507] If the business decides to accept the agreement, this action will be deemed equivalent to an order for corrective measures under Article 32 of the CPA.[508]

2. Mandatory Correction

If relevant portions of the CPA have been violated, the FTC

---

business operator in the request. *Id.* art. 29(2).

500. CPA, *supra* note 27, art. 27(4).

501. *See id.* art. 29(1). In the document containing the evaluation or authentication, the following information should be made available to the public: (1) name of the evaluator or authenticator; (2) business address; (3) scope of evaluation or authentication; (4) date of evaluation or authentication; and (5) standards and methods used. Presidential Decree, *supra* note 372, art. 31(1).

502. CPA, *supra* note 27, art. 29(1).

503. *See id.* art. 29(3).

504. *See id.* art. 29(2).

505. *Id.* art. 31.

506. *Id.* art. 31(1).

507. *Id.* art. 31(2).

508. *Id.* art. 31(3).

may order the culprit business[509] to take corrective measures to rectify the unlawful behavior.[510] The corrective measures may consist of the following:

- ceasing and desisting in the unlawful activity;
- completing of all duties and responsibilities imparted by the CPA;
- declaring that the order of correction has been received;[511] and
- other measures to be ordered on a case-by-case basis.[512]

For multiple repeated violations of the CPA, or where the business fails to comply with an order to correct the violations, the FTC may order the business to be shut down for a period not exceeding one year.[513]

3. Arbitration of Consumer Disputes

In a matter involving an alleged violation of the CPA, the FTC may order the matter to be considered by an authorized arbitrator instead of seeking voluntary correction or ordering mandatory correction.[514] If the arbitration is successful and the

---

509. The order must contain (1) the specific category and degree of violations; (2) the date and amount of specific acts comprising the violations; and (3) the extent and degree of consumer damage that resulted from the unlawful acts. Presidential Decree, *supra* note 372, art. 33.

510. CPA, *supra* note 27, art. 32(1). Violations of the following parts of the CPA are grounds for the mandatory issuance of an order to correct under Article 32(1) of the CPA: CPA arts. 5(2)–(3), 6(1), 7, 8(1) and (3) and (5), 9, 10, 11, 12(1) and (3), 13(1)–(2) and (4), 14, 15, 16(1) and (3), 17(1)–(3) and (5), 18, 19(1), 20, 22(1), 23(2), 24, 27(2) and (4), 29 (1)–(2); CPA art. 32(1)(1). Additionally, violation of any subparagraph of Article 21(1) of the CPA is a ground. *Id.* art. 32(1)(1).

511. A Presidential Decree will contain additional details regarding this item. *See id.* art. 32(3).

512. *Id.* art. 32(2)(4).

513. *Id.* art. 32(4). Table 1 of the PD contains the standards to be employed in determination of whether to suspend a business operator. Presidential Decree, *supra* note 372, art. 34.

514. *See* CPA, *supra* note 27, art. 33(1). The FTC will assist the arbitration process by provision of funds to pay the arbitration fee. *Id.* art. 33(4). Authorized arbitrators include the Korea Consumer Protection Board, the E-Commerce Mediation Committee, and others established under the consumer protection statutes. Presidential Decree, *supra* note 372, art. 35.

parties come to an agreement,[515] the FTC will then inform the parties that it will not issue or impose a mandatory order of correction.[516]

4. Penal Surcharges

If the mandatory corrective measures do not rectify the situation, and the unlawful behavior is repeated, or the measures are considered insufficient to prevent harm to the consumer, then the FTC may order a penal surcharge to be levied against the culprit business.[517] The amount of the surcharge should not exceed the sales value of the transaction in dispute.[518] However, if the amount of the sales is zero or is impossible to calculate, the assessed amount should not be exceed 50 million won.[519] Factors to consider in determining the amount of the surcharge include:

- the amount of damage to consumers due to the violations;
- the amount of compensation already given to the consumers by the culprit business firms;
- the amount of profit garnered as a result of the violations; and

515. After agreement, the parties should provide the FTC with documentary evidence of that fact. Presidential Decree, *supra* note 372, art. 36(1).

516. CPA, *supra* note 27, art. 33(2)–(3); Presidential Decree, *supra* note 372, art. 36(2).

517. CPA, *supra* note 27, art. 34(1). If imposed, the penal surcharge is in lieu of temporarily closing down the business under Article 32(4) of the CPA. *Id*. arts. 32(1)–(4). The mundane administrative aspects of late payments, installment payments, collection expenses, and payment default will be determined by Articles 55-4 to 55-6 of the Monopoly Regulation and Fair Trade Act, which are applied *mutatis mutandis* to the CPA. *Id.* art. 34(4). An FTC order should contain notice of the unlawful acts, the amount of the surcharge, and an order to pay the surcharge. Presidential Decree, *supra* note 372, art. 37(1). The penal surcharge is payable within sixty days from the date of notification. *Id*. However, if a "natural disaster, or other inevitable causes," make timely payment an impossibility, then it must be paid within thirty days after such causes cease to exist. *Id.* art. 37(2).

518. *See* Presidential Decree, *supra* note 372, art. 38 (containing detailed rules pertaining to the calculation of the amount of the surcharge as it relates to the sales value).

519. CPA, *supra* note 27, art. 34(1). Fifty million *won* is approximately. U.S. $ 49,173. Currency Converter, *supra* note 223.

- the frequency and duration of the unlawful acts.[520]

If the culprit business merges with another firm after its violation, the surviving entity will be assessed the surcharge.[521]

G. Criminal Violations

1. Refusing to Correct Violations

A party that does not respond affirmatively to an order of corrections[522] will face three years' imprisonment or a maximum fine of 100 million won.[523]

2. Unlawful Continuance of Business Operations

A party who disregards an order of business suspension[524] and continues to carry on the firm's operations will be imprisoned for a maximum period of two years or fined an amount not to exceed 50 million won.[525]

3. Grounds for Imposition of Fine of 30 Million Won

Commission of the following acts will justify a fine of 30 million won:[526] (1) failing to file a report, or filing a false report, as required by Article 12(1) of the CPA;[527] or (2) falsely indicating (for example, as with a mark) that consumer insurance is carried, or that an escrow system is allowed, in violation of Articles 24(8) and 24(9) of the CPA.[528]

---

520. CPA, *supra* note 27, art. 34(2).

521. *Id.* art. 34(3).

522. *See id.* art. 32(1).

523. *Id.* art. 40. One hundred million *won* is approximately U.S. $ 98,355. Currency Converter, *supra* note 223.

524. *See* CPA, *supra* note 27, art. 32(4); *see also id.* art 32(1) (discussing the orders of corrections).

525. *Id.* art. 41. Fifty million *won* is approximately U.S. $ 49,173. Currency Converter, *supra* note 223.

526. Thirty million *won* is approximately U.S. $ 29,503. Currency Converter, *supra* note 223.

527. CPA, *supra* note 27, art. 42(1) (amended by Act No. 7487 of Mar. 31, 2005, effective Apr. 1, 2006).

528. *Id.* art. 42(2).

4. Grounds for Imposition of Fine of 10 Million Won

Commission of the following acts will justify a fine of 10 million won: (1) provision of false information pertaining to a trade name, in violation of Article 13(1) of the CPA,[529] or (2) provision of false information pertaining to the terms of a transaction in violation of Article 13(2) of the CPA.[530]

5. Joint Punishment of a Business Firm and its Employee

When an employee of a business firm acts as the direct perpetrator under Articles 40–43 of the CPA, the perpetrator will be punished. Additionally, the business firm will be fined.[531]

6. Negligence[532]

Fines for negligence may be assessed[533] and collected[534] by the FTC or the Mayor/Do governor.[535]

High Fine

The following acts of negligence will call for imposition of a fine not to exceed ten million won:

---

529. *Id.* art. 43(1). Ten million *won* is approximately U.S. $ 9,837. Currency Converter, *supra* note 223.

530. CPA, *supra* note 27, art. 43(2).

531. *Id.*

532. This section was amended by Act No. 7487 of Mar. 31, 2005, effective Apr. 1, 2006.

533. Written notice must be given to the party containing the following: (1) the alleged acts of negligence; (2) the method of protesting the allegations; and (3) the amount of the fine if the party is found to have committed the alleged acts. Presidential Decree, *supra* note 372, art. 41(1). The party will then have at least ten days to raise oral or written objections to the allegations. If no objections are made by the party, then the party will be "deemed to have no opinion at all." *Id.* art. 41(2). In determination of the amount of the fine, the FTC or Mayor/*Do* governor will consider the motive of the party committing the unlawful acts and the effects of those acts. *Id.* art. 41(3). They will also consider the standards contained in Table 2 of the PD. *Id.* art. 42.

534. If a fine is not paid in a timely manner, the collection procedure is the same used for collection of delinquent national taxes if the fine was imposed by the FTC, or the same used for collection of delinquent local taxes if the fine was imposed by the Mayor/*Do* governor. CPA, *supra* note 27, art. 45(7).

535. *Id.* art. 45(3). Standards to be employment regarding fines are contained in the Presidential Decree. *Id.* art. 45(4).

- an issuer of settlement means[536] has failed to purchase consumer damage compensation insurance;[537]
- violating Articles 21(1)–(5-1) of the CPA;[538]
- a mail-order distributor dealing with a prepaid mail order[539] violating Article 24(2) of the CPA;[540]
- an issuer of settlement means[541] providing false data and enters into a contract of consumer damage compensation insurance;[542]
- a mail-order distributor handling a prepaid mail order[543] providing false information and entering into a contract of consumer damage compensation insurance;[544]
- sending "spam" messages;[545]
- violating the CPA by failing to attend a conference pertaining to Article 39(2) of the CPA two or more times without justification;[546]
- failing to submit a report, or the submission of a false report, under Article 39 of the CPA;[547] or
- refusing to allow inspectors to enter the worksite, or refusing to cooperate with inspection personnel.[548]

Low Fine

The following acts of negligence will justify the imposition of

536. *See id.* art. 8(4) (defining the term settlement means).

537. *Id.* art. 45(1)(1) (noting a violation of Article 24(1) of the CPA). Ten million *won* is approximately U.S. $ 9,837. Currency Converter, *supra* note 223.

538. CPA, *supra* note 27, art. 45(1)(3).

539. *See id.* art. 15(1).

540. *Id.* art. 45(1)(3).

541. *See id.* art. 8(4).

542. *Id.* art. 45(1)(2).

543. *See id.* art. 15(1).

544. *Id.* art. 45(1)(5).

545. *Id.* art. 45(1)(6) (noting a violation of Article 24(2) of the CPA).

546. *Id.* art. 45(1)(4) (noting that the procedure used is found in Article 50(10)(1) of the Monopoly Regulation and Fair Trade Act).

547. *Id.* art. 45(1)(5) (noting that the procedure used is found in Article 39 of the Monopoly Regulation and Fair Trade Act).

548. *Id.* art. 45(1)(6) (noting that he procedure used is found in Article 50(2) of the Monopoly Regulation and Fair Trade Act).

a maximum fine of five million won:

- failing to retain the records of a transaction or to facilitate the consumer's access of the records;[549]
- a business firm's failing to provide identification information to another relevant party;[550]
- failing to file a report;[551]
- failing to provide documents relating to the content of a contract or to advertise or give notice of stipulated matters;[552] or
- failing to inform a consumer that a contract for goods can be cancelled.[553]

Appeal of Fine, and Trial

A party dissatisfied with the FTC's finding of negligence and imposition of a fine may raise an objection to the FTC within thirty days from the receipt of notification of the finding.[554] Next, the FTC will then notify the adjudicating court, and the court will conduct a trial of negligence under the Non-Contentious Case Litigation Procedure Act.[555]

VII. SUMMARY, CONCLUSIONS, AND RECOMMENDATIONS

A. Recent History of Korea

The Korean Peninsula was united as an independent kingdom for much of the last 1,000 years, but it was split into two countries shortly after World War II—North Korea, a Communist government, and South Korea, a republic. The Korean War of 1950–53 was the watershed event in recent

549. *Id.* art. 45(2)(1) (noting that this would be violating Article 6 of the CPA). Five million *won* is approximately U.S. $ 4,918. Currency Converter, *supra* note 223.

550. CPA, *supra* note 27, art. 45(2)(2) (noting that this would be violating Articles 10(1) or 13(1) of the CPA).

551. *Id.* art. 45(2)(3) (noting that this would be violating Articles 12(2) and 12(3) of the CPA).

552. *Id.* art. 45(2)(4) (noting that this would be violating Articles 13(2) of the CPA).

553. *Id.* art. 45(2)(1) (noting that this would be violating Article 13(3) of the CPA).

554. *Id.* art. 45(5).

555. *Id.* art. 45(6).

history affecting the Peninsula. The North invaded the South with the help of the Chinese Army, but was repulsed by the South Korean Army, with support from the United States, British, and other forces fighting under the U.N. flag.

B. The "Tiger" on the Peninsula: Economic Growth, Computer Adeptness, and Rise of E-Commerce

Due to its anachronistic planned economic system, the North Korean economy remains underdeveloped and stagnant. On the other hand, the South Korean economy blossomed after 1980, leading South Korea to be characterized as an economic "Tiger." In the first half of this decade, an important factor in South Korea's continuing economic growth has been a marked increase in e-commerce activity. This is not surprising in view of the fact that South Korea may be the most computer-savvy nation in the world; it possesses the greatest percentage of citizens with high-speed internet connections on the planet. In its long-range economic planning, the government of South Korea has highlighted e-commerce for continued nurturing in an expectation of growth.

C. Korean E-Commerce Law

Besides the computer adeptness and internet connectivity of the South Korean people, another important driver of South Korean internet commerce—and the focus of this Article—is its e-commerce law. South Korea has enacted the "triplets"—three statutes pertaining to electronic transactions, digital signatures, and consumer protection in e-commerce. Collectively, they comprise a very sound foundation for the continued proliferation of e-commerce in South Korea. Of the three, the consumer protection statute is most deserving of praise and could well serve as a model for other countries to emulate as they develop their e-commerce laws.

1. Framework Act on Electronic Commerce

The ECA, implemented by the MCIE, set the stage. The ECA recognizes the legal validity of e-messages, provides that they may be used to comply with a statutory retention requirement, and establishes rules pertaining to their assumed

time and place of dispatch and receipt.

Even at that early stage of development of South Korean e-commerce law, consumer protections had already become an important consideration of the lawmakers. Basic consumer protections were adopted in the ECA relating to:

- confidentiality of consumer information;
- confidentiality of trade secrets;
- approval of encryption methods to increase security of e-messages;
- codes of fair consumer practices to be drafted by associations of e-commerce firms;
- establishment of a grievance process for dissatisfied consumers; and
- creation of requirements for firms to give notice to consumers regarding the firm's identity, goods and services offered, terms for the contract negotiations, the final contract, a window of opportunity to withdraw from the agreement, and document retention rules.

The ECA recognizes these basic principles for the development of e-commerce law:

- primary reliance on the private sector to implement the law using minimal government regulation but with governmental encouragement and facilitation where needed to promote e-commerce growth;
- emphasis on reliability and security in e-transactions; and
- establishment of international standards to facilitate growth in global e-commerce.

To deal with e-commerce disputes quickly and efficiently, the ECA created the E-commerce Mediation Committee. The disputing parties may voluntarily elect to have their dispute heard by this Committee. If the mediation process fails to resolve the dispute, either party may file a lawsuit in a court of law.

The ECA is open-minded to electronic signatures. The statute does not explicitly favor any one type of electronic signature but crafted the law to accept more than one type of electronic signature. Such a policy is commensurate with the international trend in e-commerce law known as "technological-

neutrality." However, because the ECA seems to encourage adoption of encryption as a security measure, this could be construed as implicit favoritism of one type of electronic signature—digital. The ECA did not address digital signatures. However, digital signatures were the focus of the DSA, the second statute of the "triplets" and the second topic in this Article.

2. Digital Signature Act

The Digital Signature Act was a companion statute to the ECA. The DSA focuses on digital signatures and is implemented by the MIC. Its purposes are to improve the reliability and security of digital signatures and increase the popularity of e-messages and e-commerce, resulting in a benefit and convenience for the South Korean people.

The DSA recognizes the legal validity of digital signatures that are supported by a certificate that has been issued by a LCA. The MIC licenses and regulates LCAs, the verifiers of the authenticity and integrity of digital signatures and the electronic records to which they are affixed. LCAs are required to draft a CPS that contains the policies, procedures, and rules they will follow in the conduct of their business. The DSA establishes specific requirements for the LCA's issuance of a certificate to an applicant, and for the LCA's suspension or revocation of a previously issued certificate. The common business operations of a LCA must be considered in the drafting of the CPS. If the LCA does not adhere to its own CPS or to any part of the DSA, the MIC may issue a corrective order to the LCA. If the LCA fails to correct the problem, the LCA's license may be suspended or revoked. Above all, the LCA must give security the highest priority. The LCA must continually strive to attain security in its computer information system, in its certificate issuance procedures, over its private key, of the subscriber's confidential information, and over its worksite.

The DSA also establishes criminal penalties for the following:

- the fraudulent use of another person's private key;
- fraudulent procurement of a certificate by giving false information to a LCA;

- aiding or abetting another in the commission of a computer crime;
- the LCA's failure to file a required document with the MIC (for example, a CPS or a report);
- the LCA's unjustified refusal to provide service, or discrimination in the provision of service;
- the LCA's failure to inform the MIC or its subscribers that it has gone out of business; and
- other unlawful acts.

The punishment may be a jail term, a fine, or both.

3. E-Commerce Transactions Consumer Protection Act

Although the two previously mentioned statutes are noteworthy, the Author considers the third statute to be the "Great Accomplishment" of South Korean e-commerce law. The CPA provides some of the best—if not the best—consumer protections for e-commerce transactions in the world. The CPA imposes criminal penalties for violations of its provisions. The CPA is implemented by the FTC. The CPA underwent a major overhaul in 2005 that became effective on April 1, 2006. This statute deserves to be considered as a model law for other nations to emulate as they develop their e-commerce law.

The purpose of the CPA is to promote the growth of e-commerce by creating a secure e-commerce environment resulting in greater confidence among consumers that the transaction will be fairly conducted. As a general rule, the CPA overrides other applicable consumer protection laws pertaining to e-commerce. If the other laws offer more consumer protection than the CPA, the more protective law applies. Thus, consumer benefit is of the utmost importance to South Korean e-commerce law.

The CPA does not cover:

- commercial buyers;
- regular, recurring, uniform transactions;
- mail-order brokers serving as middlemen; and
- other transactions.

If a seller agrees to use e-documents, they must be sent to the buyer's designated address. Easy-to-use methods must be

established allowing the buyer to change the negotiated terms before the contract is consummated. The seller should post e-documents pertinent to completed transactions at its website and allow the consumer to peruse them freely. The posted documents must include all relevant information regarding a transaction, and they must be retained securely so that no unauthorized party can obtain access to them. If e-payments are used, the seller must ensure that secure procedures are employed. Before the goods are shipped, the seller should send a confirmation to the buyer and give the buyer an opportunity to adjust the terms of the agreement or to withdraw from the agreement. If a buyer withdraws without an excuse, he may be liable to the seller for damages incurred. If a third party firm is used to deliver the goods purchased online, the firm must cooperate in dispute resolution if a grievance is filed.

The seller is never permitted to:

- convey false information to the buyer during the negotiations;
- send goods to a customer without an order and then bill the customer for the goods;
- fail to provide a new business address or telephone number;
- attempt to pressure a customer to purchase a good or service; or
- use a consumer's confidential information in any manner without his consent.

The FTC is authorized to draft additional consumer protection guidelines. If the FTC does so, e-commerce sellers must follow those guidelines. The FTC encourages e-commerce sellers to purchase consumer damage insurance for the protection of their customers. The FTC also maintains a spam refusal list, a list prohibiting the sending of unsolicited advertisements to those names on the list.

The FTC has enforcement authority that may be exercisable against business firms suspected of violating the CPA. Often, suspects are brought to the attention of the FTC by the filing of an extraordinary number of consumer complaints against them. The FTC is empowered to conduct an inspection of a suspect firm, to order correctional measures, and to impose a fine

(known as a "penal surcharge"). Additionally, the FTC may order arbitration of disputes between a business firm and a consumer, but if the arbitration process is unsuccessful, the parties may take the matter to court.

The CPA also includes criminal violations that may result in a fine, imprisonment, or both. The following are crimes which are tried in the first instance before the FTC:

- disregarding the FTC's order of business suspension and continuing to conduct business;
- failing to file a required report with the FTC, filing a false report, or falsely stating that consumer insurance is carried;
- giving false information pertaining to a trade name or the terms of a transaction;
- a corporation's violating the CPA using corporate employees as the direct perpetrator; and
- acting negligently directly or by omission.

If the guilty party is dissatisfied with the FTC's finding, he may appeal to a court of law within thirty days of receipt of the notice of the finding.

D. Recommendation: It Is Time for the World's Most Computer-Savvy Nation to Address the Online Piracy Problem

As mentioned, South Korea's e-commerce law has established a solid framework for the continuing growth of e-commerce. The ECA and the DSA are noteworthy, and the CPA provides South Korean internet buyers some of the best consumer protections in the world and deserves emulation by other nations. These three e-commerce statutes may have to be tweaked from time to time, but they are sound statutes and will not need wholesale modification in the foreseeable future. South Korean e-commerce law is in good shape.

However, it is time for the evolutionary development of South Korean internet law to enter a new phase and begin to address a new set of problems—online piracy of intellectual property. As of 2005, the International Intellectual Property Alliance (IIPA) continues to keep South Korea on the

intellectual property "Priority Watch List."[556] The following examples illustrate this continuing problem:

- online piracy by more than 1,000 culprit websites has "decimated the market for legitimate recorded music" in South Korea; sales dropped from $288 million to $162 million between 2001 and 2003, and a further fall of at least 20% was estimated for 2004;[557]
- online piracy of entertainment software, such as video games, continues almost unabated in South Korea; the Entertainment Software Association has estimated the value of pirated product in the market (valued at pirate retail prices) to be $349 million annually, with a composite (across multiple formats) piracy rate of 43%;[558] and
- online piracy of movies by more than 7700 culprit websites (a 30% increase over the 2003 figure) costs the South Korean motion picture industry a huge loss every year; and the Motion Picture Industry Association of America estimates its annual losses due to South Korean piracy at $40 million, with a video piracy rate estimated at 20%.[559]

The IIPA recommends the enactment of amendments to the Copyright Act of Korea to provide for the following:

- exclusive rights of sound recording producers;
- extension of the term of protection for intellectual property (to the life of the creator, plus seventy years);
- more stringent technological protection measures;
- increased potential liability of internet service providers;
- more limitations on rights of reproduction; and
- more emphasis on enforcement and remedies.[560]

A thorough consideration of Korea's intellectual property

---

556. International Intellectual Property Alliance, South Korea, 2005 Special 301 Report 235 (2005), at http://www.iipa.com/rbc/2005/2005SPEC301SOUTH_KOREA rev.pdf (last visited Apr. 3, 2006).

557. *Id.* at 237 (citing Russell, *South Korea Split*, BILLBOARD, Dec. 18, 2004, at 41).

558. *Id.* at 239.

559. *Id.* at 239-40.

560. *Id.* at 244-50.

laws, and proposals for amending them, is beyond the scope of this Article. Clearly, however, this will be the next big challenge for South Korea as she seeks to remain a dominant player in e-commerce.

The Author is optimistic that Korea will begin to more fully protect the intellectual creations of her artists, scientists, authors, and inventors.[561] She must. If she does not, her creators will continue to face a disincentive to produce because of diminished rewards, resulting in a long-term detriment to South Korea's output of intellectual creations and her economy.

561. Seemingly, the South Korean government realizes the seriousness of the online piracy problem and is committed to bringing it under control. However, the problem is so rampant that it may take years for this task to be accomplished. On May 3, 2004, the government unveiled its "Master Plan for IPR Protection." *Id.* at 244. Its purpose is to attain better coordination across governmental departments in dealing with the piracy problem. The Master Plan includes fifteen ways to improve Korean intellectual property law and its enforcement. *Id.*