December 2001

Impact of Cultural and Political Factors on the Adoption of Digial Signatures in Asia

Nir Kshetri
University of Rhode Island

Nikhilesh Dholakia
University of Rhode Island

IMPACT OF CULTURAL AND POLITICAL FACTORS ON THE ADOPTION OF DIGITAL SIGNATURES IN ASIA

Nir Kshetri
University of Rhode Island
nksh8805@postoffice.uri.edu

Nikhilesh Dholakia
University of Rhode Island
nik@uri.edu

Abstract

Many Asian nations have identified electronic commerce as a priority sector. Realizing that existing commercial laws – based on paper documents – do not promote Internet transactions, some Asian countries have enacted new laws to facilitate electronic commerce. Although the main technical issues associated with digital signatures and certification are well known, the cultural and political factors influencing the adoption of these technologies are not. This paper focuses attention of these cultural-political factors. While governments are aware of the commercial importance of Internet privacy and security, they are also concerned about the negative impact of encryption technology on national security, social values, and their right to rule. Our analysis indicates that adoption decisions regarding digital signature laws entail complex tradeoffs for national policy makers. In enacting such laws, Asian governments weigh the social and political costs of encryption technology against the economic benefits such technologies may provide.

Keywords: Digital signature, encryption, culture, technology adoption, Asia

Introduction

Many nations around the world realize that the development of electronic commerce is critical for their economic future. They are also realizing that laws recognizing electronic documents and digital signatures are needed to encourage Internet transactions. Digital and electronic signatures (DES), however, have been receiving only reluctant public and legal acceptance so far. By the end of 2000, only about 45 nations in the world had laws recognizing some forms of digital or electronic signatures (Stephens 2001). The issue, however, is under active consideration in many other nations.

Many Asian nations have been active in enacting new DES laws to facilitate electronic commerce. For instance, Hong Kong, India, Malaysia, Singapore, South Korea, Thailand and The Philippines have already enacted legislation to recognize digital and electronic signatures (DES). Although China does not have a specific DES law on the books, Article 11 of its Uniform Contract Law enacted in 1999 states that contracts can be written in the forms of "letters, telegrams, telexes, faxes, electronic data exchanges, and email" (Zhao 2000). In comparison to the rest of the world, so far Asian nations seem to be forging ahead in terms of recognizing digital and electronic signatures. Among the nations enacting new DES laws in Asia, however, there is no uniformity in terms of the standards for the recognition of digital and electronic signatures.

There are numerous studies examining the influence of political and cultural factors on different laws (e.g., Ahmad 2000, Fjelstad 1994, Gall 1994). Similarly, the main ideas associated with DES and certification are well known and widely disseminated. To the knowledge of the authors, however, there is no published study that attempts to relate these issues with cultural and political factors. In this exploratory paper, we attempt to fill the gap in the existing literature by providing a framework to examine the use of digital signature in a global setting. Our approach is guided by two research questions: (a) What is the spectrum of DES laws in Asia? and (b) How social, political and cultural factors influence the position of a country in the spectrum?

The remainder of the paper is organized as follows. We start with the spectrum of DES laws adoption in Asia. Then functions of signatures and their different forms are discussed. Next, DES issues are analyzed from policy and behavioral perspectives. Finally, we revisit the DES adoption situation in Asia and provide some conclusions.

Spectrum of DES Laws Adoption in Asia

In terms of the level of the adoption of electronic and digital signature, Asian nations can be divided into four groups (Table: 1). Some nations' laws do not recognize electronic signatures at all, some cover only digital signatures, while still others cover all types of electronic signatures. Likewise, some nations' laws apply to a broad range of activities, while laws in other nations are framed very narrowly, applying only to limited governmental filings or specified types of commercial transactions.

In Indonesian law, there are no specific rules or regulations about electronic signatures (Gingerich and Teo 2000). Similarly, in other developing Asian nations such as Pakistan, Sri Lanka and Vietnam, the value of e-commerce is extremely low and the governments have not yet made decisions regarding the strategies to deal with the Internet (Ebusinessforum.com 2000c, d, e). China and Taiwan are one step ahead. In Taiwan, electronic signatures have been recognized and used in filing taxes (Yang and Chang 2000). Similarly, China recognizes contracts made by Electronic Data Interchange (EDI) and e-mail (Kennedy 2000).

Economies like Korea, India and Thailand have specific DES laws. India's Information Technology (IT) Bill recognizes digital signatures. The bill, however, is not applicable to negotiable instruments, powers of attorney, trusts, wills, or any contract for the sale or conveyance of immovable property or any interest in such property (Achar 2000; Viswanathan 2000). In Korea, electronic documents with digital signatures will have the same effect of authenticity as handwritten signatures. These countries, however, do not have legal provision for the existence of certification authorities.

Hong Kong's Electronic Transaction Ordinance equates electronic messages and digital signatures to paper messages and handwritten signatures. The ordinance, however, excludes certain transactions including wills, trusts, powers of attorney, documents required to be stamped, documents concerning land, oaths, statutory declarations, judgments, court warrants and negotiable instruments (Wo 2000). Malaysia and Singapore recognize digital signatures to be as good as handwritten ones. In Malaysia, for example, if the digital signature is created in accordance with the Digital Signature Act, the effect will be the same as a handwritten signature (Wong and Chia 1999). In addition, Hong Kong, Malaysia and Singapore have legal provisions for the existence and functioning of certification authorities.

Table 1: Classification of Asian Countries by Levels of the Adoption of DES Laws (c. 2000)

Level	Characteristics	Examples
0	No legal recognition to electronic records.	Indonesia, Pakistan, Sri Lanka, Vietnam
1	Legal recognition to some forms of electronic signatures but no formal legislation to recognize digital signatures.	China, Taiwan
2	Existence of formal legislation to recognize digital signatures. Some restrictions may apply. No existence of certification authorities.	India, Korea, Thailand, The Philippines
3	Electronic and digital signatures as good as handwritten signatures. Existence of certification authorities.	Hong Kong, Malaysia, Singapore

Functions and Forms of Signatures

Signing of written documents and other formalistic legal processes serve a number of purposes.[1] When an individual signs a document, it serves as evidence and makes the contents attributable to him/her in case of dispute. A signature also expresses the signer's approval or authorization of the writing, or the signer's intention that the document should have legal effect. A signature on a written memorandum also provides a sense of clarity and finality to the transaction, improving efficiency and logistics.

Broadly speaking, signatures can be divided into two categories: handwritten signatures and electronic signatures. Electronic signatures, however, exist in a variety of forms. An electronic signature, for example, might be something as simple as a name typed at the end of an email or as sophisticated as a certified digital signature. Digital signatures or key-based digital signatures are a subset of electronic signatures, and they entail the use of specific and more sophisticated types of technologies.

[1]http://www.commerce.state.ut.us/digsig/tutorl.htm

Digital Signatures

The most common form of digital signature involves three steps: mathematical algorithms, encryption, and certification. The first step is the creation of the message digest, also known as the hash function. A mathematical formula is applied to the electronic document to create the hash. The end result is a series of characters unique to the document. The digest can be used to provide proof that the document is an original.

The second step entails the application of a special key that encrypts the digest. The key ensures that the digest can only be unencrypted by the intended recipient. This encryption process is typically done using public key cryptology. Public key cryptology (also known as asymmetric cryptology) involves two keys: one private (or secret) and one public. The keys consist of very large mathematically related numbers. The numbers are related in such a way that it is not possible to derive the private key just from the knowledge of the public key. Private key is used to encrypt messages and public key is given to the recipients so that they can decrypt the messages.

The final step – certification of the digital identity – requires a certification authority (CA). The CA checks the identification and takes steps to assure that the person getting the certificate is actually the person who he/she claims to be. By verifying the certificate of the sender and also the certificate of the CA issuing certificate to the sender, the receiver can establish data origin authentication, message integrity, and avoid the risk of repudiation.

DES from Policy and Behavioral Perspectives

Each step of digital signature – the hash function, encryption and certification – has a number of implications (Table: 2).

Table 2. Implications of the Different Steps of Digital Signature

Step	Technological	Economic	Organizational	Political	Cultural
Hash function	Complex but no need for the end-users to understand. Prepackaged software available.	Fixed computational overhead. Overall cost decreases with the increase in use.	Internal and inter-organizational authentication can be provided to a specified degree of certainty.	Government skepticism of some hash algorithms.	May be viewed as a tool of cultural imperialism in Asia.
Encryption	Complex but no need for the end-users to understand the techniques.	Inexpensive and sometimes free. Cost increases for higher level of security and performance.	Privacy and confidentiality in internal and inter-organizational messages	Governments cannot detect 'harmful' content on the Internet. Threat to authoritarian regimes.	Different view of privacy in Asia. Enables sending of pornographic contents on the Internet.
Certification	Complex networking but no need for the users to understand.	Increase in the costs of doing business. Costly to establish the infrastructure for the governments.	Organizations can establish data origin authentication, message integrity and avoid the risk of non-repudiation.	Legal provision for the liability of different parties needed. Cross-certification issues arise.	Issues related to Recognition of foreign certificates Involvement of foreigners in the CA business.

Hash Function

As Cravotta (1999) argues, "[s]ufficient security is a balance of price, performance and privacy" (p.108). Technical detail involved in the hash function is complicated and the degree of complication increases with the level of security desired. Sometimes an application may involve many algorithms working together to guarantee data integrity and authenticity. Unless users want to formulate the algorithm themselves, they do not need to understand the details of the algorithm (Cravotta 1999). Availability of prepackaged software means that clicking one key is sufficient for the end user to send a secure message. There is, however, no means to prove that an algorithm is 100 % secure. Keys are subject to attack by virus and other malicious programs (Ellison and Schneier 2000). Also, if the algorithms originate in a country that is somewhat distrusted, users and governments may have

lingering suspicions that the hash could be reversed and read by some people in the country that originated the algorithms. Inadequate technical knowledge on the part of policy makers compounds such suspicions.

Messages can be sent securely only if the sender and the receiver each maintain a secret key. Unlike email passwords, the 100-digit keys may have to be stored in a smart card rather than paper. Vulnerability of smart cards to hacker attacks is another issue. Yet another issue concerns the social complication of keeping keys secret (Kling 1993). Many individuals in an organization sometimes share passwords and it becomes semi-public instead of remaining private. Hash function can have additional risks. There is risk of collision in some hash functions and some functions may exist in unpublished form, known only to a small number of users.

Moreover, some potential users may view the use of hash function as 'another' tool of cultural imperialism and may simply be unwilling to use it. Despite these complications, hash algorithm is the most effective way to provide internal and inter-organization authentication and confidentiality of transactions with a specified degree of certainty (Tinucci 1998).

Encryption

Again, despite the technical complexity involved in the functioning of encryption software, end-users do not need to understand the detail. Sending encrypted message is only a one-click job for an end user. The software used for basic encryption is relatively inexpensive and sometimes even free. Some of the encryption software packages such as Pretty Good Privacy (PGP) are available free on the Internet. The cost, however, increases if higher-level of security is desired. Encryption is the most effective means to maintain privacy and confidentiality of internal and inter-organizational transactions.

The ability of encryption software to send messages confidentially, however, has negative political consequences and more so in an authoritarian regime. Use of encryption software makes it difficult, even impossible, for governments to detect the contents transmitted on the Internet. This has been a real threat to many control-minded authoritarian regimes of Asia, which are restricting Internet access "on the pretext of protecting the public from subversive ideas or violation of national security" (Sussman 2000, p.1). As a result, they are imposing various types of export, import, and usage restrictions on encryption software.

Authoritarian regimes operate on the presumption that everything is secret unless it is open. This is in stark contrast to the presumption in democratic countries – everything is open unless it is specifically decreed to be secret. In China, the State Bureau of Secrecy banned the discussion of "state secrets" on the Internet, and also hinted at new rules allowing only state-approved content on sites registered in China (Fang, 2000). Under China's definition, state secrets can mean "virtually any information not specifically approved for publication" (CNN.com 2000). China's new regulation requires companies to reveal the type of encryption software they use for protecting confidential information sent over the Internet, as well as the name, phone number, and E-mail address of every employee using it (Fang 2000). The new regulation also mandates that all electronic products in China use encryption software that has been created domestically (Forney et al. 2000).

Not just authoritarian regimes but also democratic governments are imposing some restrictions on encryption software. The United States government eased encryption export controls only after 1999. Exporting companies, however, are still required to report encryption exports in excess of 64-bits and are barred from selling encryption systems to Iran, Iraq, Cuba, North Korea, Libya, Syria and Sudan (Harrison 1999). A report by the Electronic Privacy Information Center (EPIC) discusses efforts by some democratic countries such as India and the Netherlands to compel users to disclose keys or decrypted files to government agencies (Gips 2000). In 1999, the government of India also warned its financial institutions that US-made security software is too weak and alerted them not to use it (Gaudin 1999).

Maintaining privacy and confidentiality is one of the major benefits of encryption technology. Government and public attitude towards privacy in Asian nations is different from that in the Western countries. For example, export restrictions on encryption software by the U.S. government were criticized on the ground that the government restricted individuals' privacy (Levin 1999). Whereas privacy is thought to be a fundamental component of democracy in the United States, many Asian nations have authoritarian political structures and/or cultural norms wherein privacy is not given the importance it receives in the West (see Hall 1966 for a classic cultural view of privacy in Asia).

Use of encryption technology is also perceived to have a negative impact on the governments' ability to control activities harmful to national, cultural, and religious values. Encryption, for example, can be used to send child pornography undetected on the Internet. In Western countries, attempts to regulate the Internet and bans on pornography are regarded as infringements of individual rights (Glass, 2000). In contrast, access to pornographic sites is banned in the Middle East and several Asian countries.

India's IT Bill, for instance, has a special section on offences dealing with the publication or transmission of "obscene material" (Achar 2000).

Instances of the use of encryption software for controversial and illegal purposes have heightened governments' suspicions of such software. In 1996, a European Commission Communication identified some areas of risk in using encryption on the Internet, including national security risks (e.g., instructions on making bombs, illegal drug production, etc) and threats to minors (e.g., abusive forms of marketing, pornography, etc.) (Price 1999). Kelley (2001) reports several examples of illegal uses of encryption software. For instance, a suspect in the bombings of the US embassies in Kenya and Tanzania in 1998 sent encrypted e-mails under various names. Similarly, another convicted mastermind of the World Trade Center bombing in 1993 used encryption software to hide the details of his plan to destroy 11 US airliners. Likewise, extremists in several countries in the Middle East, Europe and the US have been reported to use encryption software extensively for terrorist activities.

Certification

Although the networking involved in the certification process is complex, there is no need for an end user to understand the detail. But a digital certificate from a certification authority costs money. Although some CAs such as Verisign have been distributing certificates for free, such free certificates are not considered adequate for the purposes of most e-commerce transactions. In the U.S., useful certificates start at $9.95 per annum (Gibbs 1999). A majority of Internet users in Asia and elsewhere will be reluctant to spend money for something that won't have obvious and immediate value to them. Certification complements the previous two steps – hash function and encryption – to establish data origin authentication (the message in fact came from its purported sender), message integrity (the message has not been altered during transmission), and non-repudiation (the sender cannot deny that he/she sent the message) (Biddle 1997).

For effective certification, however, understanding on the part of policy makers as well as resources are needed to create the required infrastructure for certification authorities. UNCTAD (1998) points out the need for a legal infrastructure which sets out all rules and regulations pertaining to "the rights and duties of the parties, certification authorities, their liability to those who rely on good faith on the certificates they issue, criteria to be fulfilled by certification authorities and whether they should be government-controlled, accredited, licensed or freely operated commercial entities, and international recognition of certificates" (p. 23). If users do not share the same certification authority, a method must also be devised for cross-certification to make the validity and efficacy of different certificates mutually acceptable (Rutsche 1999). Other issues: Who will be responsible if one loses his/her private key? What would happen if a criminal found the CA's private key and issued digital certificates? Comparable examples, though not related to CAs, already exist in business transactions. For instance, a German court in 1999 held a bank liable for money stolen from a customer's account on the ground that the bank's encryption was not safe enough. The bank tried to shift the blame to the customer's carelessness; however, it acknowledged that in order to crack the customer's PIN number, a hacker also needed to crack the bank's 56-bit key (Levin 1999).

Given the global nature of Internet commerce, additional issues related to politics and culture arise. Should certificate issued by foreign CAs be given recognition? Should foreigners be given license to issues certificate? Asian countries differ in terms of their attitudes toward the involvement of foreigners in the business. For example, Singapore and Taiwan are pro-foreign business, but China is not (Gooley 1998).

DES Laws in Asia: Revisited

What determines the position of a country on the spectrum of DES laws (Table 1)? Economic factors matter but explain only a small proportion of the variance of the positions of different countries on the DES spectrum. Malaysia's per capita income, for instance, is much lower than that of South Korea or Taiwan, but it is far ahead of both of them in adopting DES laws. Malaysian Prime Minister Mahathir Mohamad has a reputation for making lavish investments on mega-projects such as the 88-story Petronas Twin Towers and the $3.6 billion international airport (Balfour 2000). Mahathir has the ambition to establish his country as a major player in the Internet-connected world (James 1999). Multimedia Super Corridor (MSC), his latest venture, is a $20 billion project – one of the most ambitious government projects ever undertaken in Asia (Smith 1999). Malaysia has been active in introducing e-friendly laws to attract foreign and domestic investments in the MSC.

Similarly, China is ahead of India in terms of telephone and personal computer ownership. The Chinese government, however, is "torn between its desire to create a modern telecoms infrastructure and its fear of losing control of the flow of information" (Ebusinessforum.com 2000b). The Chinese government is still finding ways to impose some measure of censorship.

Level 0

For countries in this group electronic commerce is not yet a priority sector. Indonesia, for instance, was badly hurt by the Asian financial crisis and is still struggling with its economic and political problems. Electronic commerce has not been the priority sector of the government yet (Latifulhayat 2000). Other countries in this group are relatively poorer, the volumes of e-commerce are still insignificant and the governments are not active enough. The Indonesian government has not yet analyzed the impact of different steps of digital signature on the economy. Electronic commerce is still operating in legal vacuum in these countries.

Level 1

Countries in this group have identified electronic commerce as a priority sector. They have given legal recognition to some forms of electronic records. Because of potential negative social and political impacts of encryption software, China is reluctant to accept digital signatures in "unrestricted" form. The Chinese government witnessed the negative role the electronic media played during the Tiananman Square demonstrations. The Chinese government is also aware of the role of information flow on the fall of the Soviet Union and the use of the Internet during the Soviet coup attempt. Press et al. (2000) argue that Chinese national security concerns led the government to focus its attention on the Internet before India did, which may have accelerated growth. Whereas many other countries have formal DES laws but no certification authorities, China does not have specific DES laws but the Chinese Ministry of Information Industry and the People's Bank of China are working to set up guidelines for establishing certificate authorities (Ebusinessforum.com 2000a).

Despite the higher level of economic development, Taiwan has been surprisingly slow in enacting new legislation to recognize digital signatures. Critics are complaining about the slow pace of Taiwanese government in enacting e-commerce legislation (Einhorn et al. 1999). An industry group wants the legislature to change a dozen laws and pass seven new ones regulating e-commerce. The government is considering new laws to regulate e-commerce.

Level 2

Countries in this group have identified e-commerce as a priority sector. The first and the second steps of digital signature do not pose much problem for the countries in this level. Being democratic governments, they are not much concerned about the confidential information flow on the Internet, with the exception of some restrictions concerning obscene content. There are no censorship laws in these countries as in China. Because of resource constraint or otherwise, however, they have not yet moved to the third step – establishment of certification authorities.

Level 3

Countries in this group have fully utilized all the steps of digital signature. They are economically very rich and/or have assigned very high priority to the development of Internet commerce.

Singapore is concerned about the use of encryption but has opted for different mechanisms of control. Singapore is aggressively promoting Net usage for businesses and consumers. In 1999, Singapore formed Netrust, a government agency to issue digital certificates, which is the first certification authority in South East Asia (Clarke 1999). Through smart cards and a sophisticated login system, it provides businesses and government organizations with a complete online identification and security infrastructure for secure e-commerce and other online transactions. Private companies can also seek approval from the government to issue digital certificates (Bickers 1998). In Hong Kong, the Hong Kong Post Office is the first public certification authority (Farrell and Yuen 2000).

As part of the Multimedia Super Corridor project, Malaysia has been passing legislation promoting e-commerce. Malaysian government authorized a government-owned, not-for-profit company – Mimos – to issue digital certificates (Bickers 1998). Wary of political opposition, however, Prime Minister Mahathir is imposing restrictions on Net use.

Discussion and Conclusion

An important contribution of this paper is to analyze the impact of social, cultural and political factors on the adoption of DES laws. We also discussed technological, economic, organizational, political and cultural implications of the different steps of digital signature.

While Asian governments are aware of the commercial importance of privacy and security on the Internet, they are also concerned about the negative impact of encryption technology on national security, social values and their "right to rule". Full adoption of digital signatures requires the uses of all of the three steps: hash function, encryption, and certification. The first step does not pose much problem. The second step – encryption – is inexpensive but has potentially negative influences on social, national, and political values and more so for countries with authoritarian political structures. The third step – certification – requires a good understanding on the part of policy makers and substantial commitment of resources.

References

Achar, A. "Concerns about India's new IT bill," *Telecommunications*, (34:8), 2000, p. 15.

Ahmad, K. "Islam and Democracy: Some conceptual and contemporary dimensions," *The Muslim World*,(90:1/2), 2000, pp. 1-21.

Balfour, F. "This Race is a Coup for Mahathir…But Cyberjaya is not up to Speed," *Business Week*, November 13th, 2000.

Bickers, C. "Sign in cyberspace," *Far Eastern Economic Review*, Apr 30th, 1998.

Biddle, B. "Legislating Market Winners: Digital Signature Laws and the Electronic Commerce Marketplace (Draft: 5/27/97), 1997, available at: http://www.acusd.edu/~biddle/LMW.htm.

Clarke, A. "Playing catch-up," *Asian Business*, (35:8), 1999, pp. 61-62.

CNN.com "China's Deadline for Software Registration Running Out," January 31st, 2000.

Cravotta, N. "Encryption: More than just complex algorithms," *EDN*, (44:6), 1999, pp.105-118.

Ebusinessforum.com. *BDA and The Strategies Group: China's e-commerce market will take off soon*, March 23rd, 2000a, available at: http://www.ebusinessforum.com.

Ebusinessforum.com. *China: Law and regulation,* May 4th, 2000b, available at: http://www.ebusinessforum.com.

Ebusinessforum.com. *Pakistan: Law and regulation,* May 4th, 2000c, available at: http://www.ebusinessforum.com.

Ebusinessforum.com. Sri Lanka*: Law and regulation,* May 5th, 2000d, available at: http://www.ebusinessforum.com.

Ebusinessforum.com. *Vietnam: Law and regulation,* May 9th, 2000e, available at: http://www.ebusinessforum.com.

Einhorn, B., Kripalani, M. and Shari M., "Asia Logs on," *Business Week*, February 1st, 1999.

Ellison, C. and Schneier, B. "Ten risks of PKI: What You're Not Being Told About Public Key Infrastructure," *Computer Security Journal*, (16:1), 2000, pp. 1-7.

Fang, B. "Policing Cyberspace China Sets Tough Rules," *U.S. News & World Report*, Feb 7th, 2000.

Farrell, C. and Yuen, A. "Asia Pacific moves up a gear," *International Tax Review*, 2000, pp. 24-30.

Fjelstad, P. "Legal Judgment and Cultural Motivation: Enthymematic Form in Marbury v. Madison," *The Southern Communication Journal*, (60:1), 1994, pp. 22-32.

Forney, M., Cooper H. and Bulkeley, W. M. "Government Shadow Over China's Web Grows - Spy Agency Works on Rules On Encryption," *Wall Street Journal*, January 26th, 2000.

Gall, G. "Conflict, Militancy and Crisis in Italian Industrial Relations: A Response to Terry," *Industrial Relations Journal*, (25:2), 1994, pp. 155-157.

Gaudin, S. "India Says U.S. Code a Security Risk," *Computerworld*, (33:5), 1999, p. 24.

Gibbs, M. "A Free Way to Establish Identity," *Network World*, (16:27), Jul 5th 1999, p. 58.

Gingerich, D. and Teo C. *E-com Legal Guide: Indonesia*, 2000, available at: http://www.bakerinfo.com/apec/indoapec.htm

Gips, M. A. "Home on the Page: http://www.securitymanagement.com," *Security Management*, (44:8), 2000, p. 20.

Glass, J. "Envisioning the Integration of Family and Work: Toward a Kinder, Gentler Workplace," *Contemporary Sociology*, (29:1), 2000, pp. 129-143.

Gooley, T. B. "The Changing Face of Asia: How it Affects Logistics," *Logistics Management and Distribution Report*, (37:2), 1998, pp. 45-51.

Hall, E. T. *The Hidden Dimension,* 1966, New York: Anchor Books.

Harrison, A. "Clinton Eases Crypto Export Ban," *Computerworld*, (33:38) Sep 20th, 1999.

James, D. "Politics Slow Multimedia Zone," *Upside*, (11:3), 1999, pp. 62-64.

Kelley, J. "Terror Groups Hide Behind Web Encryption Officials Say Sites Disguise Activities," *USA Today*, Feb 6th, 2001.

Kennedy, G. "E-commerce: The Taming of the Internet in China," The *China Business Review*, (27:4), pp. 34-39

Kling, B. "The Current State of Computer Science" *Bulletin of the American Society for Information Science*, (19:5), 1993, p.11.

Latifulhayat, A. "'Cyber Law' Dan Urgensinya Bagi Indonesia," Paper Presented at Seminar on "Cyber Law" Sponsored by Yayasan Cipta, Bandung, Indonesia, July 29th, 2000.

Levin, S. I. "Who Are We Protecting? A Critical Evaluation of United States Encryption Technology Export Controls," *Law and Policy in International Business*, (30:3), 1999, pp. 529-552.

Press, L., Foster, W.A. and Goodman, S.E. *The Internet in India and China, The Global Diffusion of the Internet Project*, The Mosaic Group, 2000.

Price, S.A. "Understanding Contemporary Cryptography and Its Wider Impact upon the General Law" *International Review of Law, Computers & Technology*, (13:2), 1999, pp. 95-126.

Rutsche, E. "The Long and Winding Code," *Communications International*, (26:2), 1999, pp. 36-38.

Sussman, L. R., *Censor Dot Gov: The Internet and Press Freedom 2000*, Freedom House, 2000, available at: http://www.freedomhouse.org/pfs2000/sussman.html.

Smith, G. "Yahoo, Stay Home", *Business Week*, Nov 29th, 1999.

Stephens, D. O. "Digital Signatures and Global E-commerce: Part I - U.S. Initiatives," *Information Management Journal*, (35:1), 2001, p. 68.

Tinucci, J. D. "Digital Signatures and Their Use in Treasury," *TMA Journal*, (18:2), 1998, pp. 39-42.

UNCTAD. *Electronic Commerce: Legal Consideration*, 1998, United Nations Conference on Trade and Development, Geneva, UNCTAD/SDTE/BFB/1.

Viswanathan, A. "The Bureaucratic Phenomenon in Cyberspace," *International Financial Law Review*, (19:6), 2000, 47-50.

Wong, A. and Chia, B., *E-com Legal Guide: Malaysia,* 1999, Baker & McKenzie, Singapore available at: http://www.bakerinfo.com/ apec/malayapec.htm#Telecommunication.

Wo, L. W. "Hong Kong Recognizes Digital Signatures," *International Financial Law Review*, (19:3), 2000, 35-37.

Yang, D. and Chang, H. H. *E-com Legal Guide: Chinese Taipei*, 2000, Baker & McKenzie, Taipei, available at: http://www.bakerinfo.com/apec/taipeiapec.htm.

Zhao, J. J. "Chinese Approach to International Business Negotiation," *The Journal of Business Communication*, (37:3), 2000, pp. 209-237.