<table>
<thead>
<tr>
<th>Title</th>
<th>Information highways: policy and regulation in the construction of global infrastructure in ASEAN: legal issues of the internet in ASEAN</th>
</tr>
</thead>
<tbody>
<tr>
<td>Author(s)</td>
<td>Ang, Peng Hwa</td>
</tr>
<tr>
<td>Date</td>
<td>1998</td>
</tr>
<tr>
<td>URL</td>
<td><a href="http://hdl.handle.net/10220/2905">http://hdl.handle.net/10220/2905</a></td>
</tr>
<tr>
<td>Rights</td>
<td></td>
</tr>
</tbody>
</table>
Information Highways: Policy and Regulation in the Construction of Global Infrastructure in ASEAN

Legal Issues Of The Internet In ASEAN

Ang Peng Hwa
School of Communication Studies
Nanyang Technological University
Singapore
tphang@ntu.edu.sg

Paper Presented At:
Information Highways: Policy and Regulation in the Construction of Global Infrastructure in ASEAN
November 25-27
Singapore
Asian Media Information And Communication Centre

Not to be reproduced without the author's written permission.
Abstract

This paper is an attempt to develop a comprehensive framework of legal issues and policy that have to be addressed by legislators and policy makers in order to use the new information highway. It covers the following issues: intellectual property rights, electronic commerce issues, security, privacy, content regulation, and access and service provision. The Y2K problem of computer hardware and software not recognising the Year 2000 is also mentioned.

The paper also surveys the state of readiness of ASEAN countries to e-commerce. In general, ASEAN member states are behind the curve in Internet development. There are countries that are just developing its telecommunications infrastructure. Then there are countries that are looking at the legal issues. Yet another group of countries has sufficiently developed physical and legal infrastructure to get on the information highway. But even in this third group, there are internal constraints.

The paper concludes that ASEAN governments will have to give the information highway a boost by both working on the physical as well as the legal infrastructure. (170 words)
Policy and Legal Framework

Many countries have embarked on some form of legislation to address the legal challenges in the digital environment. The countries in ASEAN are no exception. However, it is apparent that the countries are in various stages of development of their respective information infrastructure. In turn, this means that they are in various stages of development of their legislation to address their respective concerns.

This paper aims to offer a framework for an overview of the pertinent policy and legal issues in cyberspace. It is intended as a comprehensive overview. The first major challenge in addressing legislation is to understand where the legal challenges lie.

The key policy and legal issues can be grouped into six categories:

- intellectual property rights,
- issues relating to electronic commerce,
- security,
- privacy,
- content regulation, and
- access and service provision.

Another issue, which is more time-bound and, ironically, more a problem to those with wider use of computers, is the Y2K bug.

The issues are presented in the Appendix.

Brief Description Of Concerns

Intellectual Property Rights

Intellectual property rights (IPR) are probably the most significant area of concern for those involved with the new media. The area is important enough so that governments have met and continue to meet to discuss the issue.

The key concerns in this area are:

- How to manage and acquire rights in the digital environment;
- How to prevent piracy of copyrighted works; and
- How to extend the current copyright regime to include digital works.

In the international arena, the two most important developments are the Trade-Related Aspects of Intellectual Property Rights (TRIPS) agreement and the World Intellectual Property Organisation (WIPO) treaties on Copyright and Databases. The WIPO treaties were agreed on at the WIPO Diplomatic Conference in December 1996. Those were the easier parts.

A third treaty on copyright protection of multimedia and online databases, which are the harder parts, was not concluded. This means that the current IPR regime does not extend to multimedia works as a whole. Each of the components (e.g. graphics, video, music) that makes up the multimedia product has to be separately copyrighted. It is tedious for multimedia content developers to obtain permission to use or re-use the copyrighted materials from each copyright owner. The most convenient solution is a compulsory licensing scheme. Such a scheme would allow the producer to use the copyright work without first obtaining the

---

1 According to the WIPO website [http://www.wipo.org/eng/main.htm](http://www.wipo.org/eng/main.htm), as at September 10, 1998, no ASEAN country was a signatory of the treaty; Indonesia came closest as it had ratified the treaty.
copyright holder's permission. The copyright holder has a right to equitable payment for the use of his works. This approach is used in most, if not all, of ASEAN. But it is not looked upon favourably by the US and the EC and is also not in line with the direction set in the Berne Convention. Some countries are looking into the setting up of "one-stop shops" where the administration of rights over works, performances and other subject matter can be centrally managed.

In the area of trademarks, the issue of domain names on the Internet is of particular concern. How should one domain name be registered if there are valid yet conflicting claims? There is no international agreement yet on whether these cases can be considered "trademark infringement". But to be safe, companies today should register their own name as a domain name, both at internationally, in case of expansion of the business, as well as domestically.

In general, the trend is towards greater copyright protection for authors and publishers. Under the most recent WIPO agreement, the concept of "famous names" was introduced. This means, for example that if IBM is deemed a famous name, no ASEAN member should allow the registration of another company called IBM in a related activity, such as, say, a computer training school. It is probably accurate to say that ASEAN member states are attempting to balance their own national development interest (by not having a strong copyright regime) and the need to play by international rules.

**Issues relating to Electronic Commerce**

Electronic commerce on the Internet is new. So, often, current policies and law based on the traditional mode of transaction, which requires hard copy documents and signatures, and non-network mediated communication, are inadequate to address many of the issues.

In Singapore, until the passage of the Electronic Transaction Act, for example, there was uncertainty over the legal status of digital signatures, the application of contract law, and the status of digital certificates, electronic payment mechanisms and electronic payments.

Although the issues in this area are thorny, the financial rewards are attractive enough so that this area is likely to be resolved satisfactorily and soon. Lending weight to the push are the United States and the United Nations Committee on International Trade Law (UNCITRAL).

In ASEAN, much work is needed. Singapore and Malaysia are furthest ahead in amending their laws to accommodate e-commerce. Both ASEAN states have introduced legislation to admit electronic evidence in court and recognise electronic contracts.

Next in line are Thailand and the Philippines.

Thailand, through its National Electronic and Computer Technology Centre (Nectec), is drafting a set of six laws related to e-commerce that is expected to be submitted to the Cabinet by May 1999. The laws include a data protection law, computer crime/computer-related crime law, electronic data interchange (EDI) law, a digital signature law, an electronic fund transfer law and "a law to ensure that the operation of the telecommunication business and organisations would benefit the general public" (Karnjanatawe, 1998). The lack of a digital signature law is significant in Thailand because under its civil commercial code the transfer of any moveable property worth over 500 baht (US$13.50) requires the signatures of the parties (Waltham, 1998).

The Philippines in February 1998 created the Electronic Commerce Promotion Council (ECPC), a coordinating body to enhance government and private sector partnership in the promotion and development of e-commerce in the country. Among its tasks are the drafting and passage of laws to recognise electronic transactions (Malapitan, 1998).

The key concerns in this area are:
• Identification, certification and authentication of buyers and sellers, and administration of certification authorities;
• Legal status of electronic payment mechanisms and electronic payments;
• Applicability of contract law: Rights, responsibilities and liabilities of various parties and dispute resolution mechanisms;
• Fraud and crime, and law enforcement in electronic commerce;
• Money flow and taxation in electronic commerce.

The dominant theme in the concerns is to create certainty and minimise fraud and abuse. The general trend is to move towards independent third parties to create the certainty. To check fraud and abuse, hardware and software devices are used.

**Identification, Certification And Authentication Of Buyers And Sellers**

Electronic transactions depend on the ability to identify and authenticate buyers and sellers over networks, and to protect the communication between them. This requires policies and procedures for electronic identification, certification and authentication, and the administration of certification authorities (CAs). Specific questions include:

- Who can or cannot be designated certification authorities?
- Who monitor these certification authorities?
- What are the responsibilities and liabilities of certification authorities, particularly when authentication fails or when keys are compromised?

**Legal Status Of Electronic Payment Mechanisms And Electronic Payments**

Increasingly, electronic payment mechanisms such as digital cash, electronic cheques, smartcards, encrypting credit card information, and other protocols are being used. But there is some uncertainty over the legal status and administration guidelines of such payment mechanisms.

**Applicability Of Contract Law**

The extent to which offline-world-based contract law can be applied to the digital environment is questionable. Specific questions include:

- Can electronic communication expressing intent to buy qualify as an agreement "in writing"?
- When is a contract made--during payment authorisation, acceptance or fulfilment?
- What is the legal status of "clickwrap" agreements where clicking an icon on a web page is supposed to qualify as a form of "offer" or "acceptance"?

The new media also pose issues of the rights, responsibilities and liabilities of various parties and what dispute resolution mechanisms can be used. The matter is compounded by the international nature of the media: identical words can be understood differently in different countries.

**Fraud And Crime, And Law Enforcement In Electronic Commerce**

Issues of administration and enforcement, and their attendant procedures will have to be worked out. Again, because of the commercial interests of the matters, this area is likely to be resolved. There has been a first step when this year, 14 countries in North America, Europe and Australia combined to conduct simultaneous raids on suspected child-pornographers. The success of the raids suggest that if such a multi-national effort can work, smaller scale efforts should work too.
Money Flow And Taxation In Electronic Commerce

Governments will have to grapple with the inability to control money flow and taxation matters in an "invisible" economy driven by trade in information products and services. Specific questions in this area include:

- How does one assign value to and tax information products and services?
- For both tangible and non-tangible goods, given that one transaction can traverse multiple countries, who collects taxes, when and how?

No government anywhere in the world has yet worked out a scheme to tax online commerce. The US, in the belief that the absence of taxes will encourage e-commerce, has passed a law imposing a moratorium on new taxes for e-commerce. But if the volume of business activity reaches the volume projected, it is likely that the pressure and temptation to impose taxes will increase.

Security

Global networks are increasingly vulnerable to any form of virus attack, breach of security, or abuse. The many hacking incidents over the Internet attest to this. According to a 1996 US report, the US Department of Defense may have had 250,000 attacks in 1995. Perhaps even more alarming is that the precise number of attacks is only an estimate because only 1 in 150 attacks is detected (US GAO, 1996).

The systems of many ASEAN countries are probably susceptible to computer attacks. For example, Indonesian webpages were hacked following the 1998 May riots and reports of gang-rapes. The Internet vandals scrawled protested messages on websites and sent mailbombs (large mail files that fill up the mailbox and thereby prevent other mail from being sent or received) (Glave, 1998).

One answer to security has been encryption. But encryption itself raises other legal issues.

The key concerns are:

- How to protect against breaches of security in computer networks and systems;
- How to prevent crime in the digital environment; and
- Rules on the use of encryption technology.

Major software production and distribution countries like the US are introducing rules on the use of encryption technology. These rules aim to ensure that the same technology and expertise that go into protecting security are not used for unlawful purposes.

Privacy

The term "privacy" is used to refer to personal privacy, and to a lesser extent, privacy of organisations. Data protection refers to the measures taken to ensure the privacy of information.

Privacy and data protection legislation are more prevalent among the Western industrialised countries. Such privacy guidelines generally cover the following principles:

- Accountability—the organisation has to be accountable to some organisation or individual for compliance with the privacy laws;
- Identification of purposes for which the information is collected;
- Consent of person from whom data and collected, and limiting the collection, use, disclosure and retention of such data;
- Accuracy of data, which implies an error-correcting procedure;
- Openness in the procedures;
- Presence of technical safeguards to avoid inadvertent release; and
- Due process for challenging compliance--where individuals have a right to access their personal information or challenge the use of their personal information.

The key concerns are:
- How to protect against intrusion into individuals' private information;
- How to control use of personal information; and
- How to facilitate transborder data flow.

These concerns are not very different from that in the online world as the privacy principles apply equally to the new media. The additional complicating factor is the 1995 EU Directive that directs member states to adapt their legislation to address privacy and data protection concerns by 1998. The deadline has since been extended. This 1995 Directive raises issues of reciprocity because it regulates data flow to third countries. This means that while data flows within and between member states are unrestricted, member states must ensure that data flows only to third countries have "adequate protection". "Adequacy" takes into account the nature of the data, the purpose and duration of the processing operations, the country of origin and country of destination, and the laws, professional rules and security measures in the third country.

This EU Directive has grave implications for many countries because it means that countries that do not have adequate protection will not be able to obtain and process data from EU member states. In theory, the Directive covers even passenger information for airline flights. Sensibly, there are wide exemptions to allow for implied consent for transmission of the data.

Privacy is now the No. 1 concern of users on the Internet. A wise move, if personal data is collected on a site, is to include a privacy policy statement. The Economist magazine has a good privacy policy statement available at http://www.economist.com/registration/privacy.html. The American Direct Marketing Association has a webpage (http://www.the-dma.org/pan7/dmers-privacy.html) in which by clicking on the relevant buttons, it is possible to create a privacy policy.

**Content Regulation**

Most countries are trying to maintain some form of content regulation in the digital environment. They include the ASEAN countries, China, Vietnam, the US with its embattled Communications Decency Act, and the EC countries, which issued a Green Paper on the Protection of Minors and Human Dignity in the context of Electronic Services. While governments agree in principle that some content controls are necessary, disputes often arise where cultural values clash, say, free speech beliefs versus concerns about inciting hatred. The 1996 ASEAN Regulators Forum on the Internet discussing the regulation of the Internet has highlighted the fact that even among culturally similar countries, it is not possible to have a standard code.

The key concerns are:
- How to block objectionable materials on the Internet;
- How to protect national interests against undesirable materials; and
- How to reconcile conflicting cultural values in information content.

In general, governments are trying to reconcile online rules with offline rules. This means that where there is content regulation in the offline world, the same set of rules should apply if the contents move online. There is no gain or loss of rights or freedom. Such an
approach is not without problems but is a sensible first step to resolving the dilemmas created with new media.

Access and Service Provision

Access and service provision issues are less contentious in some countries compared with others, where themes such as antitrust and universal access are high on the agenda. In general, for the information highway to be widely used, telecommunication lines have to be available and costs have to sufficiently low. For example, the Philippines is working to reduce its telecommunication rates (Creed, 1998).

Such issues usually require a consideration of technology, policy and economics to resolve competing interests.

The key concerns are:
- How to manage technical standards in a networked environment;
- How to ensure interconnection and interoperability of computer systems and networks;
- How to regulate pricing and service quality of information services; and
- Responsibilities and liabilities of access and service providers.

In general, governments are sold on the idea that the new media are the wave of the future. So they are trying to encourage access. They are also trying to limit, within reasonable limits, the responsibilities and liabilities of access and service providers. In many countries, this issue is not clear. However, taking a leaf from the "Good Samaritan" provision in the US Communication Decency Act, the idea is that a provider who tries to remove illegal or libellous postings in a reasonable manner should be exempted from liability. This seems to be the most likely step that governments will pursue.

Y2K Problem

The Y2K problem is a problem caused by programming in which two digits were used to stand for the year with the "19" assumed. This means that computer programmes would assume that the year 2000 is 1900 instead. Further, the date February 29, which appears in 2000, did not exist in the year 1900 as it was not a leap year.

The precise scope of the problem is unknown. But Asia is less prepared than Western Europe or North America. Further, fixing the problem is expensive, and much of Asia cannot afford the funds to fix what many admit "may be a problem."

ASEAN Readiness

ASEAN member states are often grouped by information technology into three groups that reflect the level of computer penetration: Singapore, Malaysia, Thailand in one, Indonesia and Philippines in another that some call emerging economies and Cambodia, Laos, Myanmar, and Vietnam in the third that some call developing economies (Reuters, 1998). The different levels of computer penetration mean that there are different policy concerns and considerations.

Myanmar's rules for accessing the information highway are probably strictest among ASEAN member states. It is illegal, for instance, to own an unlicensed modem (Bardacke, 1996).

Cambodia and Laos have just started getting on the Internet. One of the Cambodia Internet access providers, CamNet, explains what the Internet is on its website http://www.camnet.com.kh/.

Telephone service is not yet universal in Vietnam. One-third of the countries communes do not have telephone service. Vietnam's state-run telecommunications company,
Vietnam Posts and Telecommunications Corp., is on an aggressive expansion plan and expects to have a total of 2 million installed in the country by the end of 1998 (Taylor, 1998). Costs in the less developed countries are expensive, especially relative to the cost of living. A Hanoi cybercafe charges 4,000 dong (US$0.30) per email message. That is the price of a meal on the street. It comes as no surprise therefore to hear the owner say that "almost 99 percent of our customers are foreign travelers" (Wired, 1998).

Indonesia has halted its ambitious telecommunications and national IT project called "Nusantara 21" because of the economic crisis sweeping the region (Leong, 1998). In practical terms, Nusantara 21 would have increased telecommunication penetration and afforded greater multimedia access. The plan appears sound and aimed to:
1. Reduce the gap between socio-economic levels in Indonesia;
2. Encourage the growth of national industry, particularly industry in information technology;
3. Assist the realization in conducting (sic) an efficient and effective government;
4. Improve education and teaching;
5. Conserve the rich national culture;
6. Encourage the growth of other sectors; and
7. Distribute information access (PT Telkom Indonesia, 1998).

In the Philippines and Thailand, the telecommunication infrastructure needs improvement and governments in both countries are working to address the problem. Malaysia and Singapore look the most ready among ASEAN states. But even in the two states, there are problems getting local banks and businesses to make it attractive to develop and use e-commerce. For example, costs involved in setting up payment mechanisms are several times higher than that in the USA.

Recommendations and Conclusion

Policy makers around the world are working to address policy and legal issues in the building of national information infrastructures. The competitive edge in the global, digital environment may well belong to those who can find clear and effective means of addressing these issues, thereby promoting the integrity of the information infrastructure. For countries to succeed in their IT plans and visions, these are important considerations.

How should the laws be introduced? There are two general approaches: one is to adopt an issue-specific set of laws. Another is to introduce a broad set of "cyberlaws" where new laws are enacted for cyberspace. Perhaps a more practical approach to "cyberlaw" is to modify or extend existing laws where possible, and draft new laws only where necessary.

In either case, it is clear that for much of ASEAN, new laws must be enacted to develop the information highway in each state. Plans must be executed. And education of businesses will also be necessary to move ASEAN on the information highway.
## Appendix

### Policy and Legal Framework

<table>
<thead>
<tr>
<th>Policy And Legal Issues</th>
<th>Brief Description Of Concerns</th>
</tr>
</thead>
</table>
| **A. Intellectual Property Rights**  
Malaysia  
Thailand  
Singapore | • How to manage and acquire rights in the digital environment  
• How to prevent piracy of copyrighted works  
• How to extend the current copyright regime to include digital works |
| **B. Issues Relating To Electronic Commerce**  
Philippines  
Thailand  
Malaysia  
Singapore | • Identification, certification and authentication of buyers and sellers, and administration of certification authorities  
• Legal status of digital signatures and digital certificates  
• Legal status of electronic payment mechanisms and electronic payments  
• Applicability of contract law: Rights, responsibilities and liabilities of various parties and dispute resolution mechanisms  
• Fraud and crime, and law enforcement in electronic commerce  
• Money flow and taxation in electronic commerce |
| **C. Security And Encryption**  
Thailand  
Malaysia  
Singapore | • How to protect against breaches of security in computer systems and networks  
• How to prevent crime in the digital environment  
• Rules on the use of encryption technology |
| **D. Privacy And Data Protection**  
Thailand  
Malaysia | • How to protect against intrusion into individual's private information  
• How to control use of personal information  
• How to facilitate transborder data flow |
| **E. Content Regulation**  
Singapore | • How to block objectionable materials on the Internet  
• How to protect national interests against foreign undesirable materials  
• How to reconcile conflicting cultural values in information content |
| **F. Access And Service Provision**  
Indonesia (suspended)  
Philippines  
Singapore | • How to manage technical standards in a networked environment  
• How to ensure interconnection and interoperability of computer systems and networks  
• How to regulate pricing and service quality of information services  
• Responsibilities and liabilities of access and service providers |
| **G. Y2K Bug** | • How to minimise possible disruptions to mission-critical operations |

Legend: Countries in black listed below the issues have some rules or policies to govern the area. Countries in grey are looking at the issues.
REFERENCES