<table>
<thead>
<tr>
<th>Title</th>
<th>New technology : legal issues</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/10220/2784">http://hdl.handle.net/10220/2784</a></td>
</tr>
<tr>
<td>Rights</td>
<td></td>
</tr>
</tbody>
</table>
New Technology: Legal Issues

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

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

The new digital environment poses many legal challenges for government, industry, and private citizen alike. The first major challenge is to understand where the legal challenges lie. This paper aims to offer a framework for an overview of the pertinent policy and legal issues in cyberspace. The key policy and legal issues can be grouped into six categories as shown in Table 1 in the Appendix below.

Brief Description Of Concerns

Intellectual Property Rights

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.

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.

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 copyright holder's permission. The copyright holder has a right to equitable payment for the use of his works. This approach is used in Singapore and other developing countries. 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. Multiple registrations of the same domain name may result in cases where the goods and services offered by the trademark owners differ, where the same trademark is registered for the same goods and services in different countries; or where the owners have exclusive rights to use the trademarks in specific countries. 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.
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. Lending weight to the push are the United States and the United Nations Committee on International Trade Law (UNCITRAL).

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 suggests 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?

**Security and Encryption**

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. The 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 and Data Protection**

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 is 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 trans border 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 generally agree that some content controls are necessary, disputes are likely to arise where cultural values clash, say, free speech beliefs versus concerns about inciting hatred.

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. 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.

Conclusion

Policy makers around the world are struggling 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.
# Appendix

## Table 1: 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**        | • 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** | • 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**              | • 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**         | • 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**                  | • 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**        | • 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                                                                                                                                          |