



On Line Governance in support of IPR Objectives

Bob Fox

Chair, Digital Economy/ICT Group EABC and JFCCT

Virtual Roundtable on Industry and Intermediary Co-operation Against online IPR infringements in Thailand

12 June 2020 1400 - 1630





SOUTH-EAST ASIA



**Virtual Roundtable on
Industry and Intermediary Cooperation
Against Online IPR Infringements
in Thailand**

- 1) On line / internet governance**
- 2) Subject Matter examples**
- 3) What is an intermediary**
- 4) Modes of Supply**
- 5) Cross border and Jurisdictional issues**
- 6) Recommendations**

- 1) On-line / internet governance**
- 2) Subject matter examples**
- 3) What is an intermediary**
- 4) Modes of Supply**
- 5) Cross border and Jurisdictional issues**
- 6) Recommendations**

There is no single law, no one national or global body covering all engagement types

Governance style varies by the subject matter area regulated
We aim to see Multi-Stakeholder Model governance, on Rule of Law principles, for all types of governance in the on-line world.

For example when it comes to IPRs, stakeholders are rights holders, intermediaries, end users/buyers/customers and government (which itself may have more than one role)

IPR impact can be relevant in subject areas not specifically about IP

Indicative governance by subject

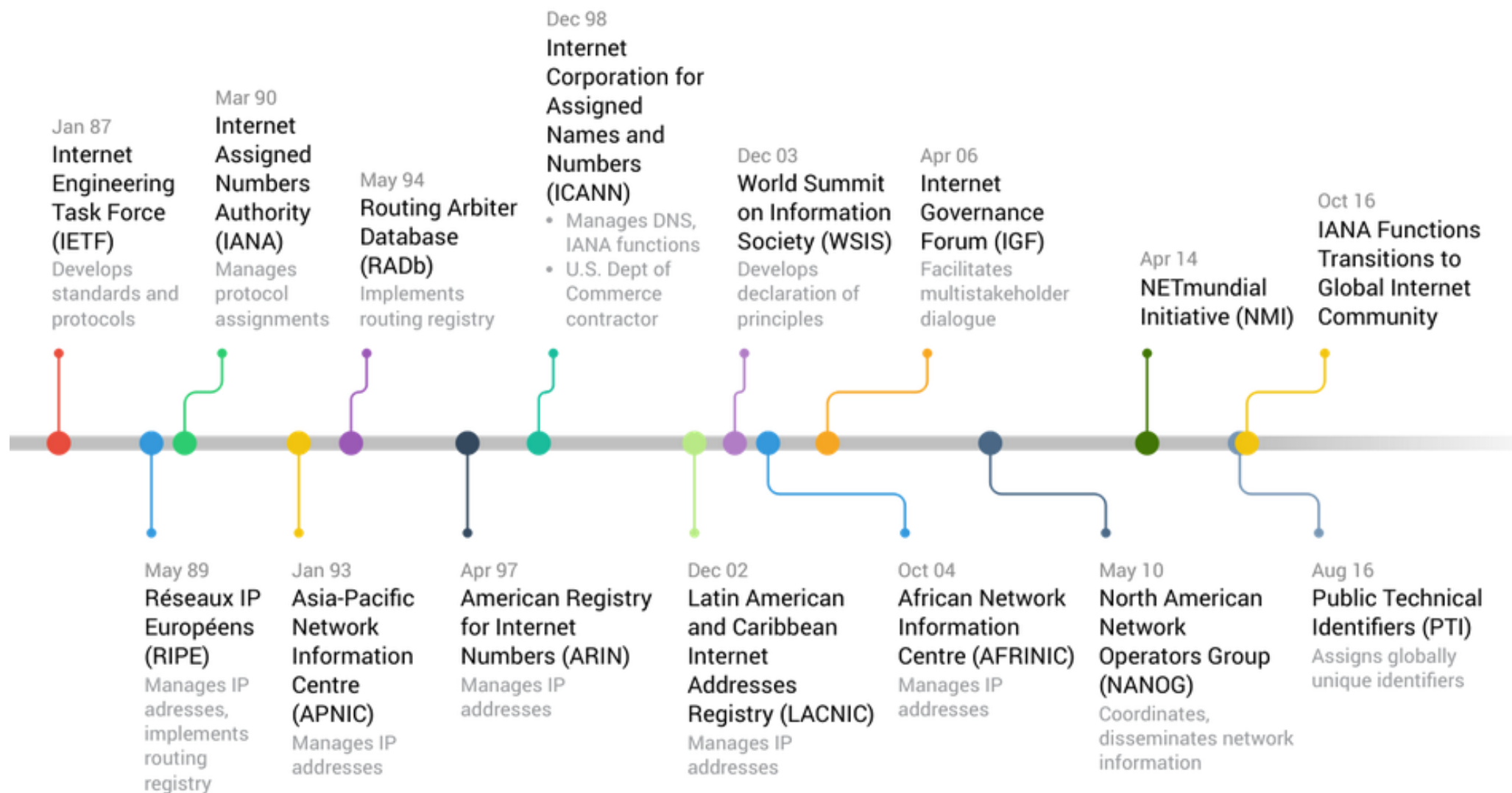
Sample Topic	TH/Other Regulatory cover – indicative
Privacy	GDPR (where relevant) PDPA from 31 May 2021; Topic specific – eg Financial records, Medical records
General internet use	Computer Crimes Act, other;
Data	Computer Crimes Act, PDPA, ASEAN instruments, GATS
Cybersecurity	Cybersecurity Act
Banking & Financial Services	Payment Systems Act, myriad of regulations
Telecomms	Frequency Act (NBTC Act); GATS Telecoms Chapter; other
eCommerce	eCommerce Act, see also EU Directive, VCPs (MoUs); Cross border also addressed in FTAs. Digital Taxes – proposed e Commerce tax (OECD co-ordination desired)
The Truth	Fake News Centre** also relevant: Defamation law
Electronic Meetings	Elegant solution in 18 April 2020 Decree BUT for technical baggage both in new Decree and old 2014 regulation (which is to be updated)
Authorisations	Electronic Transactions Act
IPRs	Computer Crimes Act (2017 Amends); Copyright Act with proposed amends
Domain Names	ICANN and related

- 1) On-line / internet governance**
- 2) Subject matter examples**
- 3) What is an intermediary**
- 4) Modes of Supply**
- 5) Cross border and Jurisdictional issues**
- 6) Recommendations**

Governance examples by subject matter

The next few slides illustrate governance examples and issues by subject matter

Internet Governance timeline



Source: Internet Governance Project, Georgia Tech. Note how IANA entered in 1990 and exited in 2016. MSM governance.

1. An essential business tool
2. A key enabler for an intelligent society

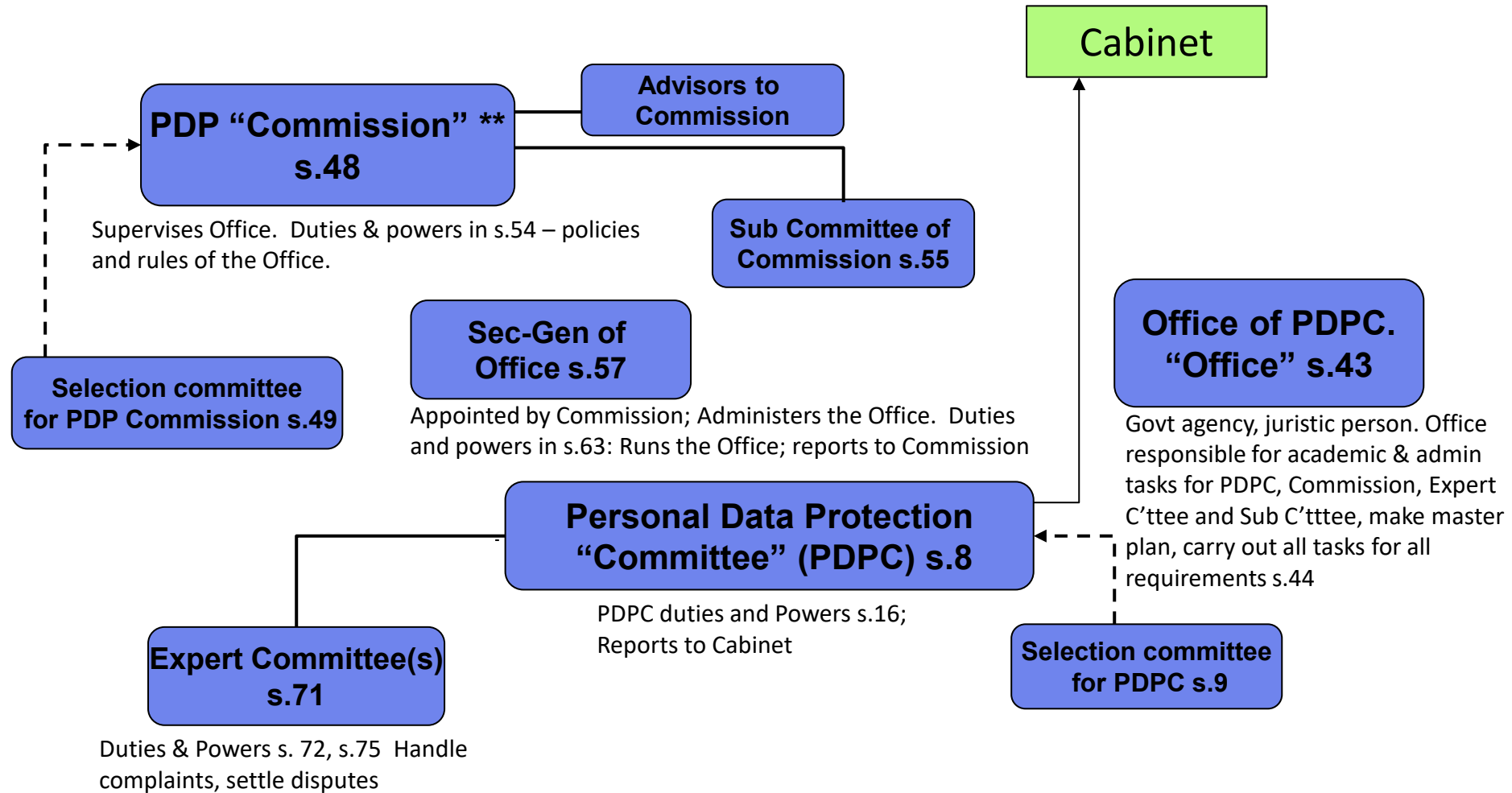
Governance: Multi-stakeholder model (MSM); top down, especially via difficult laws does not work.

Maintain an open internet while respecting privacy and supporting security. Security and Privacy are not opposite extremes

Network / operational security is everyone's job; national security should be via an agency with right Rule of Law governance

Various rights protected – privacy, IPR, security

PDPA Governance – MSM?



** PDP Commission may be called 'PDPC Supervision Committee'

The Thailand Personal Data Protection Act which has many similarities to the EU GDPR, was to have come into force in full on 27 May 2020.

But entry into force of most of the Act has been deferred to 31 May 2021. The establishment/set-up (eg Chapters 1 and 4) remain in force. The main body, the PDP Committee, has been established, with chairman + 9 experts and 6 ex-officio members including vice chair. The PDP Committee is dominated by public officials.

It remains to be seen whether the PDPA will be administered in accordance with MSM principles.

EABC has a separate file on PDP Governance.

<i>Three Roles of Government</i>	<i>What is should be</i>
Policy Maker, Rule Marker	Some critical infrastructure is in private hands. Needs multi-stakeholder model (MSM) of governance with private sector on board
User	Cybersecurity laws apply to all; Government actors should not be exonerated from complying with Personal Data Protection law or Cybersecurity law.
Operator of a Cybersecurity Command Centre	Direct management needs independence from policy making and independence from infra owners, but co-operation with private sector needed – MSM model.

Thailand's Cybersecurity Act came into force in May 2019.

To be effective, cybersecurity roles and practices need to be pervasive in the private and public sectors.

This means co-operation and buy-in not only for compliance but for rule-making and governance.

Critical Information Infrastructure (CII) is a fundamental concept in this law. CII may be public or private. But the law appears to be overly top-down rather than being built on MSM principles.

This law is a good illustration of the different roles of government.

There are many tricks to thwart IPR's; laws have developed to address these

Group / peer mindset of on-line misuse of data and other rights is not the same as applies to motion pictures (the FBI warning of criminal penalties has been used for decades). A different mindset seems to apply to part of the tech industry, where peer pressure about respecting privacy and some IPRs seems weak.

Peer responsibility mindset is evolving more slowly in some parts of the on-line world than in others.

- 1) On-line / internet governance**
- 2) Subject matter examples**
- 3) What is an intermediary**
- 4) Modes of Supply**
- 5) Cross border and Jurisdictional issues**
- 6) Recommendations**

What is an ISP? 1

In IPR parlance, an ISP is an Intermediary Service Provider (or ‘On-Line Intermediary’), ie an intermediary between rights holders and users / buyers. (Compare this with the term ‘ISP’ used in telco parlance – Internet Service Provider).

As the EABC contribution to the ISSUES BRIEF notes, what is expected of ISPs in relation to IPR objectives has become sophisticated: ISP types which are simply incapable of carrying out an action are not expected to, and would not be responsible for IPR breaches provided certain conditions are met. The Thailand Computer Crimes Act (2017 amendments) and the proposed amendment to the Copyright Act (assuming some additional regulation) bring the Thailand legal regime into line with leading world practice, including EU law.

What is an ISP? 2

The following three slides were prepared by the speaker in 2013 and developed since.

They describe the potential universe of ISPs and assess the ability of each to support ISP objectives.

As the ISSUES BRIEF notes, VCPs (refer to the two MoUs) have a ‘follow the money’ principle. As noted by this speaker at the 11-12 September 2019 IP Key Conference on Intermediaries, the payment services sector is an area which could usefully be examined for support for IPR objectives.

The statement on p. 4 in the ISSUES BRIEF “For the purposes of this paper, IPSs will be e-commerce platforms and social media’ applies to the material up to p. 6 and would not include many of the ISPs in the following three slides.

ISPs – 1 done 2013



Ref	Goods or Service provider	Normal role	Main commercial relationship(s)	Ability to control IPR infringements	Existing or conceivable remedies or actions in context of IPR infringement
1	Manufacturer	Maker of goods & supplier to wholesaler/other distributor – could also be supplier direct to retail	Component / materials providers, wholesalers or retailers	High, this is a primary infringer, infringement is intentional even if as contract manufacturer	Injunctive, damages, criminal penalties
2	Supplier of goods	Usually acts as a wholesaler - supplies goods to retail on line merchants; supplier and manufacturer could be the same person	Manufacturers, retailers	High, in most cases intentional infringement	Injunctive, damages, possible criminal penalties
3	Warehouse manager or logistics services provider; Post office	May arrange end-to-end logistics, JIT or 'as picked' supply, may also provide retail delivery services to end user; ie post sale distribution/delivery.	Manufacturers, distributors (retailers or wholesalers)	Low (eg Post office) to Medium	Injunctive – may depend on knowledge or intent; but query duty of enquiry; may rely on customer declaration about no illegal goods
4	Advertising agencies, copy producers	Provides copy, advertising and promotional services in respect of goods	On line merchant or on line market	Medium – a code of conduct could be effective in this context, but counterfeiters may not engage professionals	Injunctive – may depend on knowledge or intent; but query duty of enquiry; may rely on customer declaration about no illegal goods;

6	On line market place sites	Promotional agent for on line merchant / collective buying site – or may be the direct seller of certain goods	Suppliers, on-line merchants	High to medium – the infringement may be intentional or reckless; reliance on supplier warranty	Injunctive (eg take down order or 'remove from catalogue' order – better if able to be targeted), damages
7	Debit or Credit card issuing bank or NBFI (could be bank – typically the case with VISA/MC) or branded card NBFI issuer (eg often the case with Amex)	Provides credit or other financial services to consumer. Merchant agreement (ie authorized merchants) often done at brand (eg VISA, MC, Amex) not issuing bank level.	Consumer; card brand owner.	Very low; specific merchants can be de-authorized in the normal course.	Possible blocking order – preventing use of card or de-authorization of merchant.
8	Acquiring bank	Provides POS support	Merchant	Low to medium. It is possible (in respect of known counterfeit goods) POS system could trigger an alert for further checking – this would need an SKU level identification, and predictive or pattern-of-use or price check algorithms.	Possible blocking order – preventing supply of financial services to designated merchants.
9	Payment service provider (PSP)	Typically an NBFI – sits between bank and merchant	Bank, merchant	Low – could possibly be an agent to apply the filters subject to	Possible blocking order

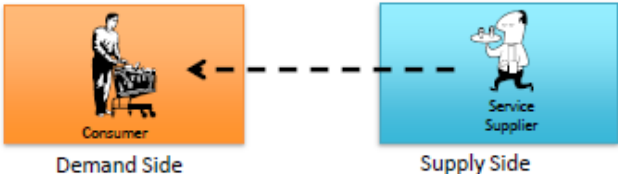
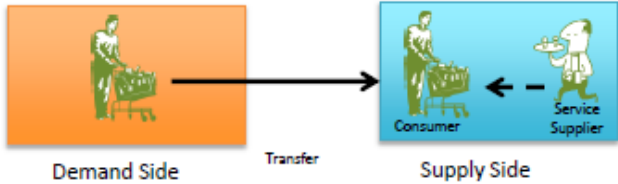
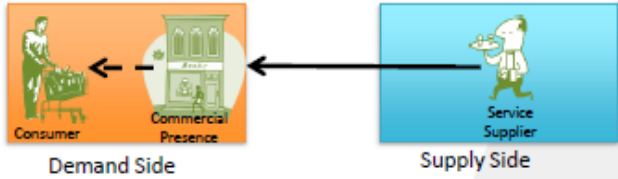
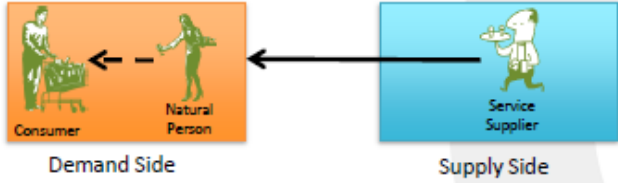
10	Electricity; UPS providers	Provide electricity to banks, on line merchants, data centres, ISPs, IP owners, manufacturers etc	Any user or electricity (ie just about every person in the value chain); gencos	Low to none	Possible blocking order to cease supply to an on-line merchant unless it ceases and desists from supplying infringing goods. Draconian step.
11	Data Centre Service Providers / other web service providers (may also include ISP function)	Hosting, co-location, web se	Merchant	Low	Injunctive (take down) – must be focused on the on-line merchant & subject to legal process
12	Internet access provider (ISP) (‘Intermediary Service Provider’ is a more recent term)	Provides access to www (the internet) via fixed wireline, fixed wireless or mobile wireless. Increasingly done by mobile operators (eg in Thailand DTC, AIS, True, TOT, TT&T,)	Consumer of internet access services; typically no relationship with www. Relies on standards (eg TCP/IP; 3GPP) to provide access.	Very low to none. Can only block access to an entire site (subject to legal process) or	Blocking order (ie to the on-line site) subject to legal process
13	Browser and search services providers	Provides management internet access tools, provide search tools, Google (eg) as a search engine flags sites on a security basis.	Advertisers, end users	Medium – certain sites can be identified (with safeguards) and tagged to alert or exclude from search results	Open to abuse – caution. Possible access denial subject to a process.

- 1) On-line / internet governance**
- 2) Subject matter examples**
- 3) What is an intermediary**
- 4) Modes of Supply**
- 5) Cross border and Jurisdictional issues**
- 6) Recommendations**

Modes of Supply - services

4 Modes of Supply of Services

Enterprise
Singapore

Modes	Forms of Service Provided
Mode 1: Cross-Border Supply Consumer and Service Supplier remain in different countries -Only the service crosses the border (E.g. An EU resident uses online services offered by a Singapore-based company)	
Mode 2: Consumption Abroad -Consumers making use of a service in another country (E.g. Tourism services; Customer from the EU travelling to Singapore to consume services from a company based here) -Also covered is the movement of consumer's property (E.g. Sending a ship or other equipment abroad for repair)	
Mode 3: Commercial Presence -Foreign companies setting up subsidiaries or branches to provide services in another country (E.g. Foreign firm from Singapore setting up a branch in the EU to provide wholesale trade services)	
Mode 4: Presence of Natural Persons -Individuals travelling from their own country to supply services in another country on a temporary basis (E.g. Salesperson from Singapore practices in EU)	

Source: Enterprise Singapore, explaining the EU-Singapore FTA

Definition of the Digital Economy



The slide following was prepared by the Digital Economy/ICT group of EABC in 2015 and updated in 2019.

The Digital Economy grows through the development of products / services which are natively digital, and by the digitized versions of analogue or off-line services. The Digital Economy also covers the on-line or digital sale and delivery of physical goods.

intrinsically digital – streaming video, eBooks, computing services, Software-as-a-Service, social media, games, various intelligent uses of Data to create value,

substitutes for established equipment and services – virtual private communications networks, security services, virtualised PBXs, Platform-as-a-Service and services delivered on-line (e.g. accounting / other business processes, graphic design, software development, data analytics, banking and financial services, on-line payments, telemedicine; industry and home automation),

marketing, sale, logistics, etc. of physical goods – (e.g. Amazon, eBay, Alibaba, Tarad.com, Lazada, Shopee),

marketing and sale of services which are not delivered on line (eg air services, taxi services, hotel bookings).

IPRs of goods and services are relevant in most cases. There are also IPRs in the platforms.

- 1) On-line / internet governance**
- 2) Subject matter examples**
- 3) What is an intermediary**
- 4) Modes of Supply**
- 5) Cross border and Jurisdictional issues**
- 6) Recommendations**

Cross Border issues

Arguably the most complex area of eCommerce (and other aspects of the on-line world) are cross border issues. They affect privacy, security, IPRs and just about every other type of on-line regulation.

Arguably the leading body dealing with cross border issues pertaining to the internet is the Paris-headquartered Internet & Jurisdiction Policy Network <https://www.internetjurisdiction.net/> It has three areas of focus: Data & Jurisdiction, Content & Jurisdiction and Domains & Jurisdiction. It aims to foster legal harmony and interoperability on these cross border issues.

The first Global Internet Report was launched at UN November 2019.

In November 2018, EABC held a conference on Privacy. The Report's author was the key speaker – see more [here](#) including booklet.



I&J – three main domains, one being content

Content & Jurisdiction

How can we manage globally-available content in light of the diversity of local laws and norms applicable on the internet?

Mainly about offensive content; less about IPRs, possibly due to relative homogeneity of IP laws (substantive) but less so for procedural laws and rules.



INFOGRAPHIC 7

Do we have the right frameworks and standards to address cross-border legal challenges on the internet?



In Thailand – for dispute resolution need to allow arbitration as well as special Courts and special skills for on-line disputes; fast track resolution.

- 1) On-line / internet governance**
- 2) Subject matter examples**
- 3) What is an intermediary**
- 4) Modes of Supply**
- 5) Cross border and Jurisdictional issues**
- 6) Recommendations**

From the ISSUES BRIEF – EABC part

Recommendation 2: Analyze in a holistic way the on-line intermediaries (ISPs) and what they can do to contribute to IPR objectives, and what each can and cannot do.

Recommendation 6: EABC supports a better understanding of on-line governance and that the best model is MSM – Multi-Stakeholder. Like privacy and cybersecurity, IPR respect and protection is a matter of public policy and to be successful requires support and engagement by many stakeholder groups including responsible government agencies, IP rights holders, intermediaries and users

Digital Literacy / Digital skills: Vital as a start to an understanding of how to play a MSM role in the on-line world. See next slide.

Digital Competencies (Digital Literacy)



Ability to use, create and share digital content safely and responsibly. It is an overarching concept for a wide range of skills:

technology competency, which is the use of digital technology;

information literacy, which is the ability to locate, identify, retrieve, process and use digital information optimally; and

media literacy, which enables us to comprehend, contextualise and critically evaluate information, as well as to create and communicate content effectively across digital media platforms.

cyber wellness, includes taking personal responsibility to use the internet for the good of the community, and understanding the risks of online dangers and negative online behaviours.

Thank you

Bob Fox

bob@fox-com.com

www.eabc-thailand.org