International
Comparative
Legal Guides

Telecoms, Media & Internet 2020

A practical cross-border insight into telecoms, media and internet laws and regulations

13th Edition

Featuring contributions from:

Arioli Law
Arnold & Porter
Ashurst Hong Kong
AZB & Partners
Bello, Gallardo, Bonequi y Garcia, S.C.
BTG Legal
CMS (UAE) LLP
Commerce & Finance Law Offices
D'LIGHT
Drew & Napier LLC
Elzaburu, S.L.P.
Fasken
Kahale Abogados
KMBK Attorneys-at-law
Krispin, Rubinstein, Blecher & Co. law firm
MinterEllison
Mobile Ecosystem Forum
Mori Hamada & Matsumoto
Morri Rossetti
Mundie e Advogados
Nikolinakos & Partners Law Firm
Pinsent Masons Germany LLP
Preiskel & Co LLP
Rato, Ling, Lei & Cortés – Advogados e Notários
RIAA Barker Gillette
Shin Associates
SOYER & SOYER/Société d'avocats
Tilleke & Gibbins
Wilkinson Barker Knauer, LLP

MEF MOBILE ECOSYSTEM FORUM
ICLG.com

Industry Chapter

Expert Chapters

Q&A Chapters

Thailand


David Duncan


Praew Annez

Tilleke & Gibbins

1 Overview

1.1 Please describe the: (a) telecoms, including internet; and (b) audio-visual media distribution sectors in your jurisdiction, in particular by reference to each sector's: (i) annual revenue; and (ii) 3–5 most significant market participants.

Thailand's two major state telecommunications operators – CAT and TOT – formerly held monopolies on telecommunications services in Thailand. Traditionally, they provided some services themselves, and they each granted concessions to private operators. The law has made a distinct shift away from the concessions regime, and replaced it with a licensing regime administered by the National Broadcasting and Telecommunications Commission (NBTC). However, some concessions still remain.

There are currently three major private mobile carriers – AIS, DTAC and True, all of which are competitors. In addition, both CAT and TOT host a number of MVNOs. Landline services are provided primarily by TOT and True, but VoIP services are a source of growing competition.

Terrestrial broadcast television has largely transitioned to digital, though some analogue broadcasters remain. As for cable and satellite television, there are several operators in the Kingdom, but the primary operator is TrueVisions.

There are numerous internet service providers, but network infra-structure is owned by a small number of major telecommunications operators (both state and private).

1.2 List the most important legislation which applies to the: (a) telecoms, including internet; and (b) audio-visual media distribution sectors in your jurisdiction.

The primary legislation relevant to telecommunications and audio-visual media distribution are:

- the Radio Communications Act B.E. 2498 (as amended);
- the Telecommunications Business Act B.E. 2544 (as amended);
- the Broadcasting Business Act B.E. 2551;
- the Frequency Allocation Act B.E. 2553 (as amended);
- the Computer Crimes Act B.E. 2550 (as amended);
- the Film and Video Act B.E. 2551 (as amended);
- the Personal Data Protection Act, B.E. 2562 (2019); and
- the Cybersecurity Act, B.E. 2562 (2019).

There is a considerable body of administrative regulations and notifications promulgated under these laws.

1.3 List the government ministries, regulators, other agencies and major industry self-regulatory bodies which have a role in the regulation of the: (a) telecoms, including internet; and (b) audio-visual media distribution sectors in your jurisdiction.

Telecommunications is primarily subject to regulation by the NBTC and the Ministry of Digital Economy and Society (MDES), including the National Information Technology Committee and the National Electronics and Computer Technology Centre. Audio-visual media distribution is primarily regulated by the NBTC, and the Censorship Board, which is a unit of the Ministry of Culture.

1.4 In relation to the: (a) telecoms, including internet; and (b) audio-visual media distribution sectors: (i) have they been liberalised?; and (ii) are they open to foreign investment?

In the telecommunications and internet space, Type 2 and Type 3 licences are unavailable to applicants considered "foreign", as determined according to the provisions of the Foreign Business Act. In addition, these licensees are obligated to observe the NBTC Notification on Prevention of Foreign Dominance. In contrast, Type 1 licences are available regardless of the level of foreign ownership in the applicant; the NBTC Notification on Prevention of Foreign Dominance is not applicable to them. Thus, foreign ownership and control is effectively limited to less than 50% for facilities-based telecommunications operators. Telecommunications operators that would operate on a non-facilities basis, however, can be wholly foreign-owned, provided they do not require a Type 2 licence for the intended services.

As for media, foreign ownership and control of a broadcasting licensee are each limited to 25%.

2 Telecoms

General

2.1 Is your jurisdiction a member of the World Trade Organisation? Has your jurisdiction made commitments under the GATS regarding telecommunications and has your jurisdiction adopted and implemented the telecoms reference paper?

Thailand has been a member of the World Trade Organization since 1 January 1995, and has made commitments under GATS regarding both value-added services and basic telecommunications.

2.2 How is the provision of telecoms (or electronic communications) networks and services regulated?

The provision of telecommunications/electronic communications networks and services is subject to the aforementioned laws, which provide for regulation primarily by the NBTC. The MDES also has a significant role in regulation.

2.3 Who are the regulatory and competition law authorities in your jurisdiction? How are their roles differentiated? Are they independent from the government?

The Trade Competition Commission and the Committee on Prices of Goods and Services are competition and fair trading regulators of general jurisdiction. These bodies are nominally independent, but the members of the Committee on Prices of Goods and Services are appointed by the government. It should also be noted that the NBTC has also issued competition regulations specific to telecommunications, as well as specific to broadcasting.

2.4 Are decisions of the national regulatory authority able to be appealed? If so, to which court or body, and on what basis?

Decisions of the NBTC can be appealed within the organisation itself, subject to the Administrative Procedure Act. Accordingly, further appeal to the Administrative Court would also be possible, depending on the circumstances.

Licences and Authorisations

2.5 What types of general and individual authorisations are used in your jurisdiction?

Primary authorisations take the form of Telecommunications Licences, which are categorised as Type 1, Type 2, and Type 3. Each Telecommunications Licence specifies the type(s) of telecommunications business in which its holder can engage, and it also typically has a range of different conditions and endorsements.

1. **Type 1 Licence**: Type 1 licences are for telecommunications operators that provide services without their own networks.
2. **Type 2 Licence**: Type 2 licences are for telecommunications operators that provide services either with or without their own networks, for use by a limited group of people, or that have no significant impact on competition, public interest, and consumers.
3. **Type 3 Licence**: Type 3 licences are for telecommunications operators that provide services with their own networks, for use by the general public or which may impact competition, public interest, or consumers.

2.6 Please summarise the main requirements of your jurisdiction's general authorisation.

Subject to certain narrow exceptions, individual authorisations – in the form of the licences described in the response to question 2.5 – are required to lawfully engage in any telecommunications business.

2.7 In relation to individual authorisations, please identify their subject matter, duration and ability to be transferred or traded. Are there restrictions on the change of control of the licensee?

The subject matter of each form of individual authorisation is described in the response to question 2.5.

Type 1 licences are valid for five years, Type 2 licences are valid for 15 to 25 years for operators with their own networks or five years for those without their own networks, and Type 3 licences are granted for periods of 15 to 25 years. Licences are renewable, subject to compliance with regulatory requirements.

Telecommunications licences are not transferable.

Public and Private Works

2.8 Are there specific legal or administrative provisions dealing with access and/or securing or enforcing rights to public and private land in order to install telecommunications infrastructure?

The NBTC administers regulations concerning rights of way for erecting poles, laying conduits or cables and installing equipment for providing telecommunications services. Depending on the type of easement required, a notice may be sufficient – otherwise, it may be necessary to negotiate an agreement. The regulation takes the general approach that such agreements should be reflective of equality, fairness and impartiality.

Access and Interconnection

2.9 How is wholesale interconnection and access mandated? How are wholesale interconnection or access disputes resolved?

There are several regulations on network interconnection and access. Essentially, licensees operating their own telecommunications networks must:

1. permit other licensees to interconnect with their networks;
2. permit other licensees to access their telecommunications networks as a means to access their networks;
3. provide transit services to other licensees through their telecommunications networks;
4. provide roaming services to other telecommunications service providers;
5. offer and provide unbundled network services and essential facilities of their own networks to permit other licensees access or interconnection with their networks; and
6. permit other licensees to access and employ technical specifications on their telecommunications network access, interfaces and protocols, or necessary technology for interoperability, in order to facilitate access or interconnection with their networks.

Licensees with their own telecommunications networks, however, may refuse to permit other licensees access to their networks if their existing telecommunications networks are insufficient to accommodate other licensees. In addition, access may also be refused if there are technical difficulties which may, as a result, cause interference in, or otherwise obstruct, the telecommunications business.

In the case of a dispute, parties may apply to the Dispute Resolution Committee of the NBTC. Detailed procedures are set out in regulations for this purpose.

2.10 Which operators are required to publish their standard interconnection contracts and/or prices?

Licensees with their own telecommunications networks are required to provide Reference Access Offers and Reference Interconnection Offers, with respect to access or interconnection by other licensees.

Licensees must also prepare information on the calculation of charges for network access, interconnection, and unbundled components. This information is to be submitted at the time of a licence application and periodically, and it is subject to consideration by the NBTC.

2.11 Looking at fixed, mobile and other services, are charges for interconnection (e.g. switched services) and/or network access (e.g. wholesale leased lines) subject to price or cost regulation and, if so, how?

Standards and pricing methodologies are set in regulations administered by the NBTC. In principle, the approach is that reasonable access or interconnection charges are to be calculated only for each network element used in providing the given service. Other expenses not directly relating thereto are not to be included in the calculation. The NBTC has the authority to order licensees to restructure their pricing, and to submit it for NBTC approval. The NBTC also has the authority to regulate each step of the procedure for access/interconnection and/or to determine network access or interconnection charges that it deems appropriate.

2.12 Are any operators subject to: (a) accounting separation; (b) functional separation; and/or (c) legal separation?

See the response to question 2.11.

2.13 Describe the regulation applicable to high-speed broadband networks. On what terms are passive infrastructure (ducts and poles), copper networks, cable TV and/or fibre networks required to be made available? Are there any incentives or 'regulatory holidays'?

As a general matter, operators of broadband networks are subject to regulation in the same way as operators of other telecommunications services, and such operators likewise generally have the same sorts of rights.

Price and Consumer Regulation

2.14 Are retail price controls imposed on any operator in relation to fixed, mobile, or other services?

Regulations administered by the NBTC impose maximum pricing for certain services.

2.15 Is the provision of electronic communications services to consumers subject to any special rules (such as universal service) and if so, in what principal respects?

Regulations impose requirements in relation to service contracts, tariffs, and service charges, as well as protection of consumer rights in the areas of personal data, privacy, and freedom of communication via telecommunications networks. Licensees are also required to establish separate call centres to receive complaints, to establish procedures for receiving and considering user complaints, and to comply with regulatory requirements in relation to handling complaints, including an escalation process in which resolution is pursued within particular deadlines.

Licensees must also meet Universal Service obligations (i.e., by making specified contributions to the Universal Service Fund).

Numbering

2.16 How are telephone numbers and network identifying codes allocated and by whom?

Telephone numbers and special codes are allocated by the NBTC, in accordance with regulations which set out, *inter alia*, a numbering plan.

2.17 Are there any special rules which govern the use of telephone numbers?

Telephone numbers can only be allocated to telecommunications licensees for use in their provision of telecommunications service, and there are extensive regulations governing such allocation. Generally, telephone numbers can only be used in providing a service consistent with the numbering plan.

2.18 Are there any obligations requiring number portability?

Mobile service users have the right to mobile number portability, and service providers are generally prohibited from acting to obstruct or impede the porting of mobile numbers to other service providers, though there are exceptions to accommodate technical and other issues. The relevant notifications set out considerable detail as to the mechanics of porting.

3 Radio Spectrum

3.1 What authority regulates spectrum use?

The NBTC is the primary regulator of spectrum use.

3.2 How is the use of radio spectrum authorised in your jurisdiction? What procedures are used to allocate spectrum between candidates – i.e. spectrum auctions, comparative 'beauty parades', etc.?

Radio frequency spectrum is allocated pursuant to the Frequency Allocation Act. For commercial spectrum usage for broadcasting, the Act provides for the NBTC to consider and grant permits for use of spectrum by auction, according to procedures and conditions the NBTC may set. As for telecommunications spectrum, the NBTC can use other methods, but auctions remain required for most commercial applications.

3.3 Can the use of spectrum be made licence-exempt? If so, under what conditions?

Certain categories of spectrum use are licence-exempt; the conditions depend on the applicable use.

3.4 If licence or other authorisation fees are payable for the use of radio frequency spectrum, how are these applied and calculated?

For commercial broadcasting use, spectrum is allocated by auction, with pricing determined by the auction process. As for telecommunications, pricing can be determined by other methods, but auctions remain required for most commercial applications.

3.5 What happens to spectrum licences if there is a change of control of the licensee?

A licensee must maintain conformity with its licence conditions in order for the licence to remain valid. In this regard, a change in control could result in breach of said conditions (e.g., if the foreign shareholding ratio was breached). Generally, a licensee must notify the NBTC in writing of a change in control, and the NBTC may instruct the licensee to take particular actions as the NBTC deems appropriate.

3.6 Are spectrum licences able to be assigned, traded or sub-licensed and, if so, on what conditions?

Pursuant to the Frequency Allocation Act, a permit to use frequency waves for a telecommunications business is the exclusive right of the permit holder and is not transferable. The holder of a permit to use particular frequencies for a telecommunications business must operate the business itself. It cannot assign management of the business, in whole or in part, to someone else, or authorise other persons to operate the business on its behalf.

4 Cybersecurity, Interception, Encryption and Data Retention

4.1 Describe the legal framework for cybersecurity.

In May 2019, the Cybersecurity Act B.E. 2562 (2019) came into force, establishing the National Cybersecurity Committee (NCSC) as well as the Office of the National Cybersecurity Committee, which will be responsible for matters regarding cybersecurity. The Cybersecurity Act also establishes the Cybersecurity Regulation Committee (CRC), which is responsible for the regulation of guidelines issued in accordance with the Cybersecurity Act, and in dealing with critical cyber threats.

The Cybersecurity Act prescribes the duties and powers of officers, state agencies, regulators, and private organisations, including Critical Information Infrastructure Organisations (CII Organisations). CII Organisations operate computers or computer systems that provide (or aim to provide) critical information infrastructure services to the public. Critical information infrastructure is defined as computers or computer systems that provide services to the public, and which belong to a government agency or a private agency, such as national security, finance and banking, energy and utilities, transportation and logistics, technology and communication, essential public services, public health, and any other areas to be prescribed by the NCSC.

A CII Organisation must protect, manage and reduce cyber risks in accordance with NCSC guidelines. The Cybersecurity Act also prescribes certain duties to CII Organisations, including the duty to provide its own cybersecurity guidelines in accordance with the NCSC guidelines, and the duty to inform the Office of the names of its officers, such as the owners, possessors, and persons responsible for monitoring computer systems. CII Organisations must also conduct cyber risk assessments by using both internal and external investigators, at least once a year.

The Cybersecurity Act sets out three categories of cyber threats: non-critical; critical; and crisis level. Non-critical cyber threats are threats that impair the abilities of computer systems used in critical information infrastructure. Critical-level threats occur when a significant increase in the threat has caused damage to computers, computer data, or computer systems used in critical information infrastructure. Crisis-level threats include threats that are more severe than the critical level and which are likely to spread to other infrastructure, and threats that could affect national security or public order.

In the case of a critical-level cyber threat, officials are authorised to take certain measures in order to analyse the situation and prevent, protect against, and lessen the risks of the cyber threat. This can include accessing the communications information of the owner, possessor or user of a computer or computer system, or the supervisor of a computer system. However, this access is limited only to where there is reasonable cause to believe that this person is related to the cyber threat or has been affected by the cyber threat, and only to the extent necessary for protection against the cyber threat.

4.2 Describe the legal framework (including listing relevant legislation) which governs the ability of the state (police, security services, etc.) to obtain access to private communications.

In principle, Thai law protects communications from access, interception and disclosure, but it provides certain exceptions for government authorities, particularly in cases that have national security implications, or cases that concern public order or good morals of Thailand. The Constitution contains provisions on privacy, which translate:

> "*A person shall enjoy the rights of privacy, dignity, reputation, and family.*
>
> *An act violating or affecting the rights of a person under Paragraph One, or the use of personal information for benefit by any means shall not be permitted, except by virtue of the provisions of the law specifically enacted as deemed necessary for the public interest.*"

In any case, in the normal course, access is available to governmental authorities through regulatory framework applicable to information technology service providers (through the Computer Crimes Act), and the regulatory framework applicable to telecommunications operators (through the Telecommunications Business Act). In addition, special powers are available to certain government officials handling certain types of cases under the Special Investigation Act, and in emergency situations, under the Emergency Decree on Public Administration in a State of Emergency. Each is explained below.

Computer Crimes Act

The Computer Crimes Act empowers competent officers of the MDES to send enquiry letters, summon concerned persons for interrogation, and request statements, documents, computer data, computer traffic data, and evidence from service providers (as defined in the Act). These officers can also order service providers to hand over certain data pertaining to users, which service providers are obligated to keep, under the law.

In addition, the officers can take further actions, but only with a court order. These include copying computer data or computer traffic data, ordering a service provider to hand over computer data, computer traffic data, or devices, examining

and accessing computer systems, computer data, computer traffic data, or devices, decrypting communications, ordering a service provider to decrypt communications, ordering a service provider to assist with decryption, and seizing/attaching a computer system, as necessary. Ministerial regulations promulgated under the Computer Crimes Act set out the specific requirements that each service provider is required to meet, in terms of data retention.

It is important to be aware that the Computer Crimes Act distinguishes between content data and non-content data. As a general matter, a court order is not required to access or obtain non-content data – a competent officer is already authorised to request such data from service providers or other relevant persons. While the Computer Crimes Act does not specifically use the term "intercept" when describing the authorities of the MDES with respect to these issues, such activities could be regarded as included within an officer's authority to examine and access computer systems, computer data, computer traffic data, or devices, as referenced above. While there is no court decision to offer guidance on this point, it is our view that a competent officer's authority extends to both stored data and those in transmission.

As noted above, the Computer Crimes Act authorises a competent officer to decrypt encrypted computer data, to order concerned persons to decrypt it, and/or to order concerned persons to cooperate with a competent officer in decrypting it, for the purposes of investigating an offence under the Act. Moreover, the Computer Crimes Act purports to apply both domestically and overseas, and compliance obligations are not only applicable to certain licensees. Rather, a competent officer has the authority mentioned above to order any concerned person to decrypt data or allow access to a computer system, among other authorities under the Act.

Telecommunications Business Act

The Telecommunications Business Act imposes certain obligations on telecommunications licensees. Through this regulatory framework, telecommunications licensees are obligated to comply with rules set by the NBTC. Licensees may also be required to arrange operations related to telecommunications activities for the benefit of public peace and order. Pursuant to regulations under this Act, telecommunications licensees are obligated to retain certain data on service users, to store it according to regulations for certain periods of time, and to provide such data to the Office of the NBTC, on request, for the purpose of supervision of the telecommunications business by the NBTC and the Office of the NBTC. While there are presently no regulations explicitly requiring standing "back doors" for easy government access to communications (whether in transit or stored), regulatory framework would accommodate the imposition of such a requirement.

Special Investigation Act

The Special Investigation Act generally applies to alleged criminal violations of certain laws, which are unusually complex, relevant to national interests, involve influential people or certain officials, or cases otherwise selected by the Special Case Board. With respect to data interception or access, the Special Investigation Act requires Special Case Inquiry Officials to obtain a court order prior to access or acquisition of any documents or information in transmission through various means of communications which have been or may be used to commit a Special Case Offence (as defined in the Act). Under this Act, the competent officer would need to file a petition requesting the court to issue an order authorising such access or acquisition of data.

Emergency Decree on Public Administration in a State of Emergency

The Emergency Decree, *inter alia*, provides for expanded investigative powers usable in the event of an emergency declaration made by the Prime Minister. This Decree gives broad powers to the Prime Minister to act in virtually any way necessary to maintain public order or otherwise maintain control in emergency situations. In such event, the Prime Minister can, among other actions, authorise a competent official to issue an order to inspect any means of communication or issue a notification prohibiting any act or instructing the doing of anything necessary for maintaining the security of the state, the safety of the country or the safety of the people (this is sufficiently broad to include interception of or access to data, as deemed necessary).

Order 3/2558 of the National Council for Peace and Order

Governmental access can also be authorised pursuant to broad authorities existing under Order 3/2558 of the National Council for Peace and Order (NCPO).

Non-compliance under any of the foregoing can result in fines, imprisonment, and/or seizure of equipment, depending on the violation.

4.3 Summarise the rules which require market participants to maintain call interception (wire-tap) capabilities. Does this cover: (i) traditional telephone calls; (ii) VoIP calls; (iii) emails; and (iv) any other forms of communications?

Telecommunications licensees are not under a general requirement to maintain or enable interception capability. Nevertheless, regulatory framework would accommodate the imposition of such technical requirements, if such a policy decision were made. Moreover, current law enables officials to order a telecommunications licensee (or any other person) to carry out or to cooperate with interception so ordered. Such order could be issued in respect of any form of communications.

4.4 How does the state intercept communications for a particular individual?

In normal circumstances, with probable cause, the state may apply to the Chief Justice of the Criminal Court for an order permitting interception of communications of any individuals, whether through wiretapping or monitoring of written and/or electronic communications. Such requirements, however, may be circumvented through special procedures under some of the laws described in our response to question 4.2 above, such as the Emergency Decree or NCPO Order 3/2558.

4.5 Describe the rules governing the use of encryption and the circumstances when encryption keys need to be provided to the state.

Encryption can be regulated under multiple laws.

With respect to telecommunications applications, the Radio Communications Act provides for the regulation of activities relating to radio communication in Thailand. The Act prohibits any person from producing, possessing, using, importing, exporting, or trading in any radio communication equipment, unless such person is granted a licence by the NBTC. It provides authority for the NBTC to issue notifications to exempt particular types of radio communication equipment, or those used in certain activities, in either case, as a class or on an individual basis. To the extent any item constitutes radio

communication equipment, if encryption capabilities exist in such devices, they would be subject to regulation as part of the device. To date, we are unaware of any denial of approval of a device on the basis of encryption functionality.

With respect to military applications, the Armaments Control Act B.E. 2530 (as amended) provides for regulation of the importation, bringing in, manufacturing, and/or possession of any armament. It provides that no person shall import, bring in, manufacture, or possess armaments, except where a licence has been obtained from the Secretary of Defence, or where an exemption is applicable. The definition of armaments can be construed quite broadly, and it even includes several routine items that happen to have military applications (dual-use). As such, to the extent that encryption technology, or equipment or software which includes encryption technology is considered an "armament", a licence would be required to import it or otherwise bring it in to Thailand. We are, however, not aware of this law ever being used to deny the importing/bringing in or possession of routine equipment or software used for computer networking and/or telecommunications applications.

Also, the Computer Crimes Act authorises officials of the MDES to access computer systems to decrypt encrypted computer data, order concerned persons to decrypt such data, and order concerned persons to cooperate with a competent official in decrypting such data, for the purposes of investigating an offence relevant to the Computer Crimes Act.

4.6 What data are telecoms or internet infrastructure operators obliged to retain and for how long?

Pursuant to regulations issued under the Telecommunications Business Act, telecommunications licensees must retain certain personal data of telecommunications users, including the facts and details concerning each service user by which the service user can be identified, service usage data, telecommunications numbers, and descriptions of individual usage. Licensees must keep personal data of their service users for the last three months (counted from the day following the current day), and in the event that the service is terminated, retain such data for three months following the date of termination of the service. In the case of necessity, the service provider may be required to retain the data for longer than three months after termination of service, but not for longer than two years.

The Regulations issued under the Computer Crimes Act also contain similar obligations that are applicable to service providers (as defined in said Act). Service providers include telecommunications licensees and some operators that are not telecommunications licensees. The Act requires service providers to retain necessary information on each service user, as well as specified computer traffic data; the type of computer traffic data varies by type of provider and/or service. The required computer traffic data must be stored for at least 90 days from the date the data is entered into the computer system, unless extended by a competent official. A competent official may extend this beyond 90 days, but for no more than two years, in particular cases. In addition, service providers must keep user identification data so that the service user can be identified from the beginning of use of the service, and the service provider must keep this data for at least 90 days after termination of the service.

5 Distribution of Audio-Visual Media

5.1 How is the distribution of audio-visual media regulated in your jurisdiction?

Distribution of television is handled pursuant to the Broadcasting Business Act, with the NBTC as the primary regulator. Other forms of audio-visual media, such as DVDs and computer games, are outside the scope of that Act, but other laws are relevant to them. Notably, the Film and Video Act provides regulatory framework for cinema and DVDs.

The NBTC has been particularly active in exercising its authority with respect to content and competition issues. In multiple cases, the NBTC has fined operators for the broadcast of what was regarded as inappropriate content. It has also intervened in the market to provide for free broadcast of certain sporting events, to address competition concerns.

5.2 Is content regulation (including advertising, as well as editorial) different for content broadcast via traditional distribution platforms as opposed to content delivered over the internet or other platforms? Please describe the main differences.

The Broadcasting Business Act provides for regulation of the content of television programmes that are broadcast. Content requirements (including advertising) vary between terrestrial broadcasting and non-frequency broadcasting (e.g., cable or IPTV), as well as between different categories of channels.

In addition, the Film and Video Act provides for content controls in respect of movies, commercials, television programmes, videos, certain videogames, karaoke, and other similar content. A committee constituted under that Act has the authority to censor such content, requiring changes before their release.

There are currently no regulations specific to OTT services accessible via the public internet. Generally, operators are subject to the same restrictions regarding content requirements and censorship as traditional distribution platforms. However, it should be noted that there are mechanisms for blocking websites or parts of websites, as under the Computer Crimes Act, the Emergency Decree, NCPO Order 3/2558, and the Constitution.

5.3 Describe the different types of licences for the distribution of audio-visual media and their key obligations.

The Broadcasting Business Act and regulations promulgated thereunder establish the framework for: (i) broadcasting network licences; (ii) broadcasting service licences; (iii) broadcasting facilities licences; and (iv) broadcasting application service licences.

Broadcasting service licences are issued for broadcasts using frequencies (e.g., free-to-air) and not using frequencies (e.g., cable). For broadcasts using frequencies, there are multiple categories of licences for public and community broadcasting, but these are available only to government entities and certain associations, foundations, charities, and educational institutions. With respect to commercial services, these can be licensed at the national, regional, or local levels. Non-frequency broadcasting services are licensed separately. With respect to frequency and non-frequency commercial broadcasting licences, foreign ownership in the licensee is limited to 25%.

Other regulatory requirements deal with the directorship of companies holding the licences (i.e., that at least 75% of the directors be Thai nationals). Analogous ownership and control restrictions apply to licensees that exist as partnerships. Broadcasting licensees are subject to several other regulatory requirements, some of which exist in law and regulations, and others that are imposed through licence conditions.

5.4 Are licences assignable? If not, what rules apply? Are there restrictions on change of control of the licensee?

Licenses are not transferable. However, a licensee may allocate time slots for programming of others, subject to further regulatory requirements.

A licensee must maintain conformity with its licence conditions in order for the licence to remain valid. In this regard, a change in control could result in breach of said conditions (e.g., if the foreign shareholding ratio was breached). Generally, a licensee must notify the NBTC in writing of a change of control, and the NBTC may instruct the licensee to take particular actions as the NBTC deems appropriate.

6 Internet Infrastructure

6.1 How have the courts interpreted and applied any defences (e.g. 'mere conduit' or 'common carrier') available to protect telecommunications operators and/or internet service providers from liability for content carried over their networks?

According to the Computer Crimes Act, any service provider that cooperates, agrees, or conspires in relation to a specified offence involving a computer system under its control is subject to the same penalty as that imposed upon the person committing the offence, provided that where the service provider has complied with the regulatory notification setting out something largely analogous to a "mere conduit" defence, the service provider shall not be subject to penalty. It is likely that strict compliance with the notification would be necessary in order for a service provider to avail itself of the defence.

6.2 Are telecommunications operators and/or internet service providers under any obligations (i.e. to provide information, inform customers, disconnect customers) to assist content owners whose rights may be infringed by means of file-sharing or other activities?

The Copyright Act B.E. 2537 (as amended) addresses obligations of internet service providers in relation to infringing content, providing a mechanism by which one can petition the court to request that infringing content be taken down.

Also, pursuant to the Computer Crimes Act, service providers could be held liable in respect of illegal content on their networks, unless they have acted in conformity with the "mere conduit" regulation. Among the requirements of that regulation, a service provider must have a mechanism for receiving complaints/take-down notices, and for acting on them. The Computer Crimes Act also provides a mechanism by which service providers can be ordered to block/remove illegal content.

6.3 Are there any 'net neutrality' requirements? Are telecommunications operators and/or internet service providers able to differentially charge and/or block different types of traffic over their networks?

Regulations provide that licensees are under general obligations to operate their telecommunications network services and provide services to service users and interconnection users on a non-discriminatory basis. However, they do not go so far as to explicitly require net neutrality.

6.4 Are telecommunications operators and/or internet service providers under any obligations to block access to certain sites or content? Are consumer VPN services regulated or blocked?

Pursuant to the Computer Crimes Act, following the issuance of a court order, a competent official under the Computer Crimes Act may block particular websites or other content, or order ISPs to do so. Blocking of websites or content is also possible under the Emergency Decree and NCPO Order 3/2558. As for VPN services, the provider thereof would be regulated as a service provider under the Computer Crimes Act which, as noted above, requires the retention of specified user data. Access to VPN services has been blocked on occasion, but they are generally available.

David Duncan is a consultant in the Tilleke & Gibbins corporate and commercial group, specialising in technology, media, and telecommunications, antitrust/competition law, and projects. In the TMT space, which comprises the largest part of his practice, David has extensive experience in structuring and negotiating IT outsourcing transactions, developing structures by which to offer new telecommunications and/or IT services in Thailand, handling TMT-related M&A transactions, advising on IT infrastructure projects, and advising on regulatory implications of all the foregoing. He also has particular expertise in government contracting. His client base is foreign and domestic, and he advises new entrants to the market, as well as established operators. David is ranked in the TMT category by *Chambers Asia-Pacific* and *Legal 500*, and he has also been recognised by *Chambers* and other publications for projects expertise.

Tilleke & Gibbins
Supalai Grand Tower, 26th Floor
1011 Rama 3 Road
Chongnonsi, Yannawa
Bangkok 10120
Thailand

Tel: +66 2056 5555
Email: david.d@tilleke.com
URL: www.tilleke.com

Praew Annez is a consultant in Tilleke & Gibbins' corporate and commercial department. She assists associates and partners on a wide range of corporate and commercial matters, including energy industry matters and anti-competition regulations. She regularly advises clients on technology, media and telecommunications, data protection, and anti-corruption compliance.

Tilleke & Gibbins
Supalai Grand Tower, 26th Floor
1011 Rama 3 Road
Chongnonsi, Yannawa
Bangkok 10120
Thailand

Tel: +66 2056 5510
Email: praew.a@tilleke.com
URL: www.tilleke.com

Tilleke & Gibbins is a leading regional law firm in Southeast Asia with over 150 lawyers and consultants practising in Bangkok, Hanoi, Ho Chi Minh City, Jakarta, Phnom Penh, Vientiane, and Yangon. Our firm represents the top investors and the high-growth companies that drive economic expansion in Asia in the key areas of commercial transactions and M&A, dispute resolution and litigation, and intellectual property.

Our TMT practice handles all aspects of work in this field and enjoys an international reputation. Our success on our clients' behalf has led to global recognition as a leading TMT practice by such publications as *Chambers Asia-Pacific*, *The Legal 500 Asia Pacific*, *Asialaw Profiles*, and others.

www.tilleke.com

Tilleke & Gibbins

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Finance & Leasing
Aviation Law
Business Crime
Cartels & Leniency
Class & Group Actions
Competition Litigation
Construction & Engineering Law
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Recovery & Insolvency
Corporate Tax
Cybersecurity
Data Protection
Digital Health
Drug & Medical Device Litigation
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Financial Services Disputes
Fintech
Foreign Direct Investment Regimes
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Sanctions
Securitisation
Shipping Law
Telecoms, Media & Internet
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by:

global legal group