

# Thailand



**Veeranuch Thammavaranucupt**



**Sappawit Jansuparerg**

Weerawong, Chinnavat & Partners Ltd.

## 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.**

The estimated market value of the telecommunications sector in Thailand in 2019 was approximately THB 605 billion. The most significant market participants in each sector are as follows:

- Mobile network operators: AIS; True; and dtac.
- Landline services: TOT; True; and CAT.
- Fixed broadband internet services: True; 3BB; TOT; and AIS

In the broadcasting sector, the estimated annual revenue in 2019 was approximately THB 77 billion. Most terrestrial broadcasting services have changed to digital services. There are many active market participants, both state enterprises and private operators. The major national operator in cable and satellite broadcasting is True. Certain fixed broadband internet operators are also providing broadcasting services via broadband networks (“IPTV”), for example, AIS.

**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 and any significant legislation on the horizon such as the regulation of online harms or artificial intelligence (please list the draft legislation and policy papers).**

The National Broadcasting and Telecommunications Commission (“NBTC”) – established under the Act on the Organization to Assign Radio Frequency and to Regulate Broadcasting and Telecommunications Services B.E. 2553 (2010) (as amended) (the “**Frequency Act**”) – is the main regulator for telecommunications, internet and broadcasting services in Thailand.

The main laws in relation to telecommunications and broadcasting services are:

- Frequency Act.
- Telecommunications Business Act B.E. 2544 (2001) (as amended).
- Radio Communications Act B.E. 2498 (1955) (as amended).
- Broadcasting and Television Businesses Act B.E. 2551 (2008).
- Film and Video Act B.E. 2551 (2008) (as amended).
- Consumer Protection Act B.E. 2522 (1979) (as amended).
- Foreign Business Act B.E. 2542 (1999) (as amended).

- Act on Commission of Offences Relating to Computers B.E. 2550 (2007) (as amended).
- Trade Competition Act B.E. 2560 (2017).
- Personal Data Protection Act B.E. 2562 (2019).
- Cybersecurity Act B.E. 2562 (2019).

In 2019, the Cybersecurity Act and Personal Data Protection Act were enacted to address online harms.

The Thai government has deferred the enforcement of most provisions of the Personal Data Protection Act for one year (to become effective on 1 June 2021) in order to provide additional time for public and private sector entities to prepare their internal processes and to ease the financial burden they are shouldering during the COVID-19 pandemic.

**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 (including internet) and broadcasting services are generally regulated by the NBTC.

In addition, the Censorship Board of the Ministry of Culture may ban audio-visual media content that is not in compliance with its notifications. Reasons for censorship range from violation of moral and cultural norms to disturbing the public order and national security.

**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 including in relation to the supply of telecoms equipment? Are there any upper limits?**

Telecommunications (including internet) and broadcasting services have become liberalised by virtue of the Constitution of the Kingdom of Thailand B.E. 2540 (1997) which established an independent regulatory body (now the NBTC) responsible for allocating radio frequencies, regulating radio and television broadcasting and other telecommunications businesses for the benefit of the public and to create a level playing field among market participants.

Previously, telecommunications and broadcasting services were exclusively provided by the state under a monopolistic scheme. As time went by, the Thai government liberalised these services to accommodate the surging demand and exponential development of communications in the digital era. While some concessions continue, the legal mechanism for the operation of telecommunications services has transitioned from the concession regime to the licensing regime.

At present, the NBTC is the key regulator. Any person wishing to operate telecommunications and broadcasting services must apply for a certain licence or concession from the NBTC accordingly.

Subject to certain exemptions and depending on the business model, the supply of telecommunications equipment is generally subject to foreign business restrictions under the Foreign Business Act B.E. 2542 (1999) (the “**FBA**”) which is the main legislation regulating business conducted by foreigners in Thailand. Foreigners wishing to operate restricted businesses must obtain a foreign business licence or foreign business certificate from the Ministry of Commerce.

## 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 (“**WTO**”) since 1 January 1995, with certain commitments (i.e. *GATS/SC/85 and GATS/SC/85/Suppl.2*) to the major principles of the WTO in relation to basic telecommunications services.

Accordingly, all new legislation in relation to communications was required to be in force as of 2006, as well as public telecommunications services carried out in accordance with the regulations issued by virtue of those relevant acts.

The liberalisation of the Thai telecommunications market and the promulgation of the relevant laws and regulations noted above demonstrate compliance with such commitments.

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

The provision of telecommunications (including electronic communications) networks and services is regulated under the licensing regime in which the NBTC functions as an independent regulator.

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

There are two agencies responsible for overseeing the competition landscape in the telecommunications and broadcasting sectors.

The first agency is the NBTC. The second agency is the Trade Competition Commission which was established under the Trade Competition Act B.E. 2560 (2017) as an independent entity with quasi-judicial authority for the enforcement of competition law in all sectors, in coordination with sector regulators.

Licensees in the telecommunications and broadcasting sectors are required to comply with the specific legislation and regulations of the NBTC and, in the absence of an NBTC regulation in certain areas of competition law, they are required to comply with the Trade Competition Act and its subordinate regulations.

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

In general, decisions of the NBTC can be appealed to the Administrative Court if the person affected by such decision takes the view that the decision of the NBTC does not comply with the law.

### Licences and Authorisations

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

Individual authorisation (i.e. licence) is primarily implemented in Thailand. General authorisation may be in the form of an exemption that is limited to certain services, for example, the provision of internet and telephone services that are managed by a business operator and implemented solely for the facilitation of its hotel business.

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

If the services to be operated fall within the exemption as specified under the relevant NBTC notification, there is no need for the business operator to apply for a licence.

**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?**

In general, any person who wishes to operate a telecommunications business in Thailand is required to obtain a licence:

- **Type 1 Licence:** Business operators that do not have a telecommunications network and meet the characteristics deemed appropriate to provide services on the basis of liberalisation.  
*Application:* Submitted to the NBTC.  
*Validity period:* No expiry date.
- **Type 2 Licence:** Business operators that have or do not have a telecommunications network and intend to operate a business to provide services for a limited group of people or a business that will have no significant impact on free and fair competition or no significant impact on public interest and consumers.  
*Application:* Submitted to the NBTC.  
*Validity period:* No expiry date.
- **Type 3 Licence:** Business operators that have a telecommunications network and intend to operate a business to provide services to the general public or a business that may have significant impact on free and fair competition or significant impact on public interest or requires special consumer protection.  
*Application:* Submitted to the NBTC.  
*Validity period:* 15–25 years (this period may be adjusted by the NBTC).

Licences are granted on an exclusive basis and cannot be transferred or sub-licensed to a third party.

In the case of a merger between licensees, the licensee, who (i) wishes to merge with another, or (ii) would receive benefits from the merger, is required to submit a request or notify the NBTC

within a certain period of time before or after such merger (as the case may be) as prescribed by the relevant NBTC notification.

**2.8 Are there any particular licences or other requirements (for example, in relation to emergency services) in relation to VoIP services?**

There is no particular licence or requirement (other than those that apply to the licensee) in relation to VoIP services in Thailand. If the licensed VoIP services require the use of a telecommunications number, the licensee is required to comply with the NBTC notification on the allocation and management of numbering.

However, the NBTC has the authority to prescribe additional licence conditions.

## Public and Private Works

**2.9 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?**

Provisions for administering and enforcing the right of way to public and private land for the installation of certain telecommunications infrastructure/equipment (excluding customer premises equipment) are included in the Telecommunications Business Act B.E. 2544 (2001) (as amended) and relevant NBTC notifications.

In order to install telecommunications infrastructure/equipment and exercise a right of way, the licensee must submit a request to exercise such right to the NBTC, together with a diagram illustrating the details of the directions and boundaries for the installation of the infrastructure/equipment and its relevant accessories, for prior approval.

When NBTC approval is granted, the licensee may proceed with the installation of its telecommunications infrastructure/equipment. The public or private landowner is entitled to charge certain fees at the rates determined by NBTC notifications.

## Access and Interconnection

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

The main regulation governing mandatory interconnection and access, as well as the dispute resolution mechanism, is NBTC Notification Re: Telecommunications Access and Interconnection B.E. 2556 (2013) (the “**Notification on Access and Interconnection**”).

Additionally, NBTC Notification Re: Domestic Roaming governs the mandatory domestic roaming services; and NBTC Notification Re: Infrastructure Sharing for Mobile Network B.E. 2556 (2013) governs the mandatory access to a radio network and its facilities.

■ **General requirements for mandatory wholesale interconnection**

Licensees that have a network shall have the following duties, among others:

- (1) Offer and arrange to have their network interconnected with other licensees who have a network and request interconnection on a fair, reasonable and non-discriminatory basis.

- (2) Provide the correct and necessary information concerning the network interconnection to the other licensees that have a network and request interconnection.
- (3) Negotiate and finalise the terms and conditions of the interconnection agreement within a reasonable time.
- (4) Offer and provide unbundling network services and essential facilities for their own telecommunications network in order to permit other licensees’ interconnection with their network.
- (5) Provide adequate signal transmission circuits and the necessary network interconnection equipment at points of interconnection, such that licensees requesting network interconnection are able to provide services of good quality.
- (6) Permit other licensees to interconnect and employ technical specifications on telecommunications network access, interfaces and protocols or necessary technology for network interoperability in order to interconnect with the network.
- (7) Not to take any action which may prevent other licensees from regular interconnection with the telecommunications network, or which may cause interference or interruption to the telecommunications business.

■ **General requirements for mandatory access**

- (1) Provide the correct and necessary information concerning network access to other licensees that have a network and request interconnection.
- (2) Negotiate and finalise the terms and conditions of the network access agreement within a reasonable time.
- (3) Offer and provide unbundling network services and essential facilities for their own telecommunications network to permit other licensees’ access to their network.
- (4) Not to take any action which may prevent other licensees from regular access with the telecommunications network, or which may cause interference or interruption to the telecommunications business.

Nonetheless, a request to interconnect and access the telecommunications network may be refused in certain scenarios such as the case that the existing telecommunications network capacity is insufficient to accommodate other licensees; and technical difficulties in the telecommunications network interconnection that may cause interference or obstruction to the telecommunications business.

■ **Initial dispute resolution**

The Notification on Network Access and Interconnection provides the initial dispute resolution mechanism whereby the Dispute Resolution Committee has the authority to conduct dispute resolution as it deems appropriate with fair treatment to all parties.

However, if a party disagrees with the decision of the Dispute Resolution Committee, an appeal may be made to the NBTC.

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

A licensee that owns a telecommunications network is required to publish the reference interconnection offer which must include, among other information, the terms and conditions of interconnection and the interconnection prices.

**2.12 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?**

The NBTC has announced a referenced price for the interconnection of both fixed and mobile services. This price has been typically implemented among licensees.

The interconnection charge must be fair, reasonable and non-discriminatory among the licensees and must be calculated by long run incremental cost methodology (“LRIC”). The access price shall be as agreed between parties provided that such charges must be fair, reasonable and non-discriminatory among the licensees.

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

There is no law requiring legal or functional separation. However, the NBTC requires the telecommunications business licensees having significant market power or designated licensees to prepare and submit a separate accounting report for each type of telecommunication business (including separation of telecommunications operations from non-telecommunications operations).

**2.14 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’?**

The local loop unbundling and network access regulations for high-speed broadband networks are the same as described above.

There are no incentives or ‘regulatory holidays’ for high-speed broadband networks.

## Price and Consumer Regulation

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

Yes, the NBTC sets out the regulations controlling the maximum price of retail telecommunications services (e.g. voice, SMS, mobile broadband, fixed broadband) as well as the pricing structure of domestic mobile services.

**2.16 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?**

Licensees are also required to contribute certain fees to the Universal Service Obligation Fund as prescribed by the relevant NBTC regulations. The key principle of the Universal Services Obligation is to provide universal service supply for basic telecommunications services covering both spatial and social dimensions with the aim of mitigating the problem of the digital divide within the country.

The provision of telecommunications services to consumers is also subject to various laws in relation to standard contract, consumer protection, pricing control and data privacy.

## Numbering

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

The NBTC is responsible for the allocation of telephone numbers and network identification codes in accordance with its regulations and numbering plan.

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

There are extensive regulations concerning the use of telephone numbers, e.g. the use of international access numbers with service codes, short numbers, toll-free numbers, telecommunication numbering allocation, telecommunication numbering plan and allocation of rare telephone numbers.

A request for allocation of a number will be first considered by the Sub-Committee on Telecommunication Numbering and will be subject to NBTC approval.

**2.19 Are there any special rules relating to dynamic calling line identification presentation?**

In general, a dynamic calling line identification service is not available for individual customers in Thailand. However, a corporate customer may employ dynamic calling line identification to the extent that the dynamic numbers used are within the range to which such corporate customer subscribed.

**2.20 Are there any obligations requiring number portability?**

The NBTC requires licensees that are mobile network operators to accommodate mobile number portability services among mobile network operators and to establish a clearing house for mobile number portability.

## 3 Radio Spectrum

**3.1 What authority regulates spectrum use?**

Spectrum use is regulated by the NBTC.

**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.?**

The Frequency Act provides that any person wishing to use a radio spectrum for broadcasting for commercial purposes must obtain a licence from the NBTC, usually by auction. Nonetheless, the NBTC may implement other allocation procedures, in addition to an auction, for allocating spectrum which are for: (i) bandwidth where there are many spectra; (ii) public services; (iii) national security; or (iv) other non-profit businesses.

**3.3 Can the use of spectrum be made licence-exempt? If so, under what conditions? Are there penalties for the unauthorised use of spectrum? If so, what are they?**

The use of certain spectra is exempt from licensing requirements

as listed in the NBTC Notification Re: Frequency and Radio Communication Equipment Authorized for General Use.

A person who uses an unauthorised spectrum shall be liable to a fine and/or imprisonment or both as the case may be.

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

In addition to spectrum allocation fees, in most cases, in accordance with the spectrum auction rules, the spectrum licensee is required to pay annual frequency usage fees in accordance with the ministerial regulation of the Ministry of Information and Communication Technology Re: Frequency Usage Fees.

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

The spectrum licensee is usually the telecommunications or broadcasting business licensee and must maintain the qualifications and conditions required by the NBTC. Any change in control may trigger certain requirements to prepare a filing for NBTC approval or acknowledgment as the case may be.

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

In general, the spectrum licences are granted on an exclusive basis where the licensee cannot transfer or sub-license its rights to any third party, unless the licensee has received approval from the NBTC and the assignment fees have been duly paid.

## 4 Cyber-security, Interception, Encryption and Data Retention

### 4.1 Describe the legal framework for cybersecurity.

At present, the main legislation governing cybersecurity in Thailand is the Cybersecurity Act B.E. 2562 (2019) (the “CSA”) which became effective on 28 May 2019. The CSA provides a legal mechanism against any cyber threat, which is broadly defined as any unlawful action or undertaking by using a computer, computer system, or undesirable program with an intention to cause harm to a computer system, computer data, or other relevant data, and includes imminent threats which would cause damage or affect operation of a computer, computer system, or other relevant data.

The committees established by the CSA include the National Cybersecurity Committee which is responsible for laying down overall policies while the Cybersecurity Supervision Committee monitors and regulates compliance with the CSA.

The CSA categorises cyber threats into three levels; the authority of the relevant committee over governmental agencies and/or private entities would be different depending on the level of cyber threat: (i) non-critical level; (ii) critical level; and (iii) crisis level.

The CSA applies to critical information infrastructure organisations (“CII Organisation(s)”), which may be either public or private sector entities carrying out the following tasks or services:

- (1) National security.
- (2) Material public service.
- (3) Banking and finance.

- (4) Information technology and telecommunications.
- (5) Transportation and logistics.
- (6) Energy and public utilities.
- (7) Public health.
- (8) Other areas that may be further prescribed by the relevant cybersecurity authority.

CII Organisations have the following obligations:

- (1) Provide the contact information of the owner(s), person(s) in possession of, and operator(s) of computers.
- (2) Comply with the code of practice and maintain cybersecurity standards.
- (3) Procure risk assessments for cybersecurity.
- (4) Implement certain mechanisms or procedures to monitor and resolve any cyber threats or incidents relating to the CII Organisation.
- (5) Notify the relevant officials regarding any cyber threats.

Failure to comply with these obligations under the CSA is subject to a fine and/or imprisonment.

If a cyber threat occurs, under the order of the National Cybersecurity Committee, *any* person is required, depending on the severity of the threat, to: (i) provide access to the relevant computer data or computer system, or other information related to the computer system; (ii) monitor the computer or computer system; and (iii) allow officials to test or cease the operation of the computer or computer system and/or seize a computer, a computer system, or any equipment. In doing so, a court order is required, with the exception of cases where the official deems that a crisis level cyber threat has occurred.

### 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.

The right to privacy is a fundamental right enshrined in the Constitution of Thailand. While interpersonal communications must be protected from access, interception, and disclosure, the protection is limited to those that are not contrary to national security, public order or good morals. In light of this, the governmental authorities may impose certain legal measures to obtain access to private communications under the following legislation:

#### (1) Criminal Procedure Code

Under the Criminal Procedure Code, the main legislation for criminal proceedings, the inquiry official, i.e. the police, may obtain access to private communications for the purpose of collecting evidence.

#### (2) Cybersecurity Act B.E. 2562 (2019)

As addressed in question 4.1.

#### (3) National Intelligence Act B.E.2562 (2019 (the “NIA”))

The NIA empowers the National Intelligence Agency to order any government agency or person to handover data and devices that have an impact on national security. If such person fails to comply with the order without appropriate grounds, an order from the Prime Minister may be obtained. If necessary, the National Intelligence Agency may proceed with any measure (i.e. including employing electronic, scientific or telecommunications devices or other technologies) to obtain information or documents regarding an intelligence operation, counter-intelligence operation, communications intelligence operation, or civilian security.

#### (4) Prevention and Suppression of Involvement in Transnational Crime Organisation Act, B.E. 2556 (2013)

The investigating officer, authorised by the Attorney General, National Police Commissioner-General, or other

authorised person, as the case may be, may submit a request to the Chief Justice of the Criminal Court for the issuance of an order to obtain a document or information if there is a reasonable cause to believe that such document or information delivered by post, telex, telephone, facsimile, computer, communication tools or equipment, electronic media or any technological media is used or may be used to derive benefit from the commission of an offence of involvement in a transnational criminal organisation.

**(5) Computer Crime Act, B.E. 2550 (2007) (as amended) (the “CCA”)**

The CCA authorises competent officers, upon obtaining a court order, to inspect, access and/or copy a computer system, computer data, computer traffic data or computer data storage equipment for the purposes of the investigation of potential crimes under the CCA and Penal Code to the extent necessary. The authority of the competent officers is broadly defined and may be interpreted to include the interception of private communications.

**(6) Special Case Investigation Act B.E. 2547 (2004) (the “SCI Act”)**

The SCI Act would apply to complicated criminal cases or special case offences, such as cases concerning national security, influential persons or officials, or cases selected by the Special Case Board.

The Special Case Inquiry Officials, established under the SCI Act, may access and acquire any documents or information transmitted via any means of communication which has been or may be used for committing a special case offence. Prior to the execution of such power, a court order must be obtained.

**(7) Telecommunications Business Act B.E. 2544 (2001) (as amended) (the “TBA”)**

Although the TBA generally protects telecommunications business licensees from any access, interception or disclosure by a third party, it does include a provision for authorities to take possession of and use a device or equipment of any licensee if it becomes necessary to maintain public order or national security.

**(8) Order of the National Council for Peace and Order No. 3/2558 (2015) Re: Maintaining Public Order and National Security (“NCPO Order No. 3/2558”)**

The objective of NCPO Order No. 3/2558 is to maintain public order and national security, thus, it bestows extensive power to peacekeeping officers in order to prevent and suppress any offences in relation to *lèse majesté*, national security, the law on firearms, and any other orders issued by the NCPO.

Peacekeeping officers have certain powers to seize any equipment or devices in order to obtain access to private communications.

As a side note, the power of the peacekeeping officers is currently held by the police.

**(9) Notification of the National Council for Peace and Order No. 26/ 2557 (2014) Re: Supervision and Surveillance on the Use of Online Social Media (“NCPO Notification No. 26/2557”)**

Pursuant to NCPO Notification No. 26/2557, the Online Social Media Committee has the power to examine, scrutinise, and access any online information. In addition, it has the power to suspend or close online publications, websites and social media platforms on numerous grounds, such as causing incitement of hostility, undermining the integrity of the law or credibility of the NCPO.

In addition to the foregoing legislation, there are other laws empowering the relevant authorities to obtain access to private communications, such as the security exchange law, anti-money laundering law, anti-human trafficking law, prevention and suppression of narcotics law and law on public administration in emergency situations.

**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?**

There are no explicit regulations requiring telecommunications business licensees to maintain call interception capabilities.

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

In general, a court order is required to intercept the communications of an individual. Nonetheless, there are certain situations addressed in question 4.2 for which a court order is not a prerequisite for urgent and necessary interceptions.

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

For the purpose of investigation, if there is probable cause to believe that there is a potential offence under the CCA, or a request by the relevant officer, the competent officer is authorised to acquire evidence to identify the allegation and prove an offence. In light of this, the competent official has the power to obtain a court order in order to access a computer system, computer data, computer traffic data or a computer data storage device and to decrypt the computer data of any person.

**4.6 Are there any specific cybersecurity requirements on telecoms or cloud providers? (If so, please list the relevant legislation.)**

There are no specific requirements imposed on telecommunications or cloud providers under the cybersecurity laws in Thailand. Nonetheless, these services are ‘technology and telecommunications’ businesses and may be considered as CII Organisations under the CCA accordingly.

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

There are two laws that require telecommunications and/or internet infrastructure operators to retain a logfile:

■ **The TBA**

Certain personal data of telecommunications users including the factual information or details which may be directly/indirectly identifiable to: (i) the individual user; (ii) usage details; (iii) subscribed number; and (iv) behavioural activity in using telecommunications services must be retained by the licensee for three months. The foregoing data must be retained for three months from the termination of service. If necessary, the licensee may retain the data for

longer than three months after the termination of service, but not exceeding two years.

#### ■ The CCA

A service provider must maintain traffic data for a period of no less than 90 days from the date on which such data was entered into the computer system. If necessary, the competent official may, on a case-by-case basis, order any service provider to maintain computer traffic data for a period longer than 90 days but not exceeding two years. In addition, the service provider must keep the user data as necessary for identification of the user from the first day of such service and store such user's data for a period not less than 90 days from its expiry date.

## 5 Distribution of Audio-Visual Media

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

The primary legislation specifically regulating the broadcasting business is the Broadcasting and Television Businesses Act, B.E. 2551 (2008) (the “**Broadcasting Act**”). The NBTC is the primary regulator:

- (1) setting out licensing requirements and allocating the radio frequency spectrum for a business operator, and overseeing the compliance of the licensee;
- (2) overseeing compliance with the managerial requirement for broadcasting and television stations;
- (3) preventing anti-competition arrangements;
- (4) regulating broadcasting and television programmes;
- (5) promoting and controlling the professional ethics of the licensee and the relevant personnel; and
- (6) supervising the establishment, utilisation, and connectivity of a broadcasting and television network.

In addition, audio-visual media (e.g. films, videos, advertisements, videogames and karaoke) is regulated under the Film and Video Act B.E. 2551 (2008). The Censorship Board has the authority to review and consider whether content may be distributed. This act also regulates certain distribution activities for audio-visual media such as the export of audio-visual media from Thailand and the sale or exchange of audio-visual media within Thailand.

### 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.

Content broadcasting through frequency distribution platforms and non-frequency distribution platforms such as IPTV are both subject to the requirements on content type allocation under the Broadcasting Act.

In addition, if any content does not comply with the restrictions prescribed by the NBTC, the NBTC has the authority to suspend the distribution platform. Content is also subject to the Film and Video Act B.E. 2551 (2008) as described above.

In respect of over-the-top (“**OTT**”) services, there are currently no specific regulations on the content of such services distributed through the internet. Nonetheless, NCPO orders and notifications govern the censorship and blocking of prohibited content, photos, video footage from any internet platforms including OTT services.

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

The licences for audio-visual broadcasting, i.e. television businesses as prescribed under the Broadcasting Act are based on the use of frequency, including the licence for a television business using a frequency and the licence for a television business that does not use a frequency.

For television businesses, there are three types of licences:

- (1) a licence for public service operations;
- (2) a licence for community service operations for the fulfilment of communal needs; and
- (3) a licence for business service operations for the purpose of generating income.

The licence for public service operations and the licence for community service operations are reserved for government entities, certain non-profit organisations and higher education institutions, whereas the licence for business service operations is available to private entities.

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

The licences and rights in connection with television businesses are granted on an exclusive basis and cannot be transferred or sub-licensed to any third party. Nonetheless, the licensee may allocate airtime to other persons in order to broadcast their programmes under certain criteria.

Any change of control may trigger the requirements to prepare a filing for NBTC approval.

## 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?

Any service provider who abets or aids the perpetration of certain offences by using the computer system under its control shall be liable for the same penalty as the offender under the CCA or other laws.

Generally, there is no law providing an exemption for liability for such offences nor has the court rendered an interpretation concerning an available defence (e.g. mere conduit or common carrier) for the service provider.

### 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?

According to the Copyright Act B.E. 2537 (as amended), in the case where there is reliable evidence demonstrating copyright infringement in the computer system of a telecommunications operator and/or an internet service provider, the copyright owner may submit a petition requesting the court to order the service provider to cease such copyright infringement.

In addition, under the CCA, any service provider who collaborates in, gives consent to or knowingly overlooks certain offences in a computer system under its control shall be held liable, unless such service provider can prove that it has been proceeding in compliance with the relevant regulation. The competent officer may obtain a court order to block access or 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?**

While there is no express provision on 'net neutrality', telecommunications operators and/or internet service providers are required to provide their services on an equal and non-discriminatory basis.

**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?**

The competent officer may obtain a court order to block access or remove illegal content under the CCA. Further, under certain circumstances (e.g. political unrest, severe emergency situation), to maintain public order and national security, the government may suspend, block, or remove any site or content which it deems necessary.

VPN service providers are subject to provisions of the CCA, as these services fall under the definition of a 'service provider' provided therein. Access to VPN services may be blocked in certain circumstances, on the basis of a court order.



**Veeranuch Thammavaranucupt** leads the Capital Markets and Corporate Governance Practices. She has considerable experience in capital markets and mergers and acquisitions, particularly innovative transaction structures and telecommunications in both domestic and cross-border transactions. Veeranuch is recognised as a leading lawyer by *The Legal 500*, *IFLR1000*, *Asialaw Profiles* and *Chambers and Partners*. Prior to joining the Firm, she was general counsel at a major telecommunications and internet services company in Thailand.

**Weerawong, Chinnavat & Partners Ltd.**  
22<sup>nd</sup> Floor, Mercury Tower, 540 Ploenchit Road  
Lumpini, Pathumwan  
Bangkok 10330  
Thailand

Tel: +662 264 8000  
Email: [Veeranuch.t@weerawongcp.com](mailto:Veeranuch.t@weerawongcp.com)  
URL: [www.weerawongcp.com](http://www.weerawongcp.com)



**Sappawit Jansupareg** advises public and private companies in a wide array of strategic transactions, including mergers, acquisitions, joint ventures and corporate restructurings as well corporate and commercial matters. In addition to his substantial experience in the telecommunications industry, Sappawit has represented companies across a broad range of industries, including technology, private equity, venture capital, manufacturing, medical and transportation.

**Weerawong, Chinnavat & Partners Ltd.**  
22<sup>nd</sup> Floor, Mercury Tower, 540 Ploenchit Road  
Lumpini, Pathumwan  
Bangkok 10330  
Thailand

Tel: +662 264 8000  
Email: [Sappawit.j@weerawongcp.com](mailto:Sappawit.j@weerawongcp.com)  
URL: [www.weerawongcp.com](http://www.weerawongcp.com)

Weerawong C&P, one of Thailand's leading law firms, combines local legal expertise with international standards of excellence. Solution-oriented, commercially minded, and driven by results, we offer a full range of legal services to local and international clients doing business in Thailand, ASEAN and around the world.

[www.weerawongcp.com](http://www.weerawongcp.com)

**WEERAWONG C&P**  
WEERAWONG, CHINNAVAT & PARTNERS LTD.