Chambers AND PARTNERS

CHAMBERS GLOBAL PRACTICE GUIDES

TMT 2025

Definitive global law guides offering comparative analysis from top-ranked lawyers

Indonesia: Law and Practice

Agus Ahadi Deradjat (Agung), Mahiswara Timur, Nina Cornelia Santoso and Natasya Nurul Amalia
ABNR Counsellors at Law

INDONESIA

Law and Practice

Contributed by:
Agus Ahadi Deradjat (Agung), Mahiswara Timur,
Nina Cornelia Santoso and Natasya Nurul Amalia
ABNR Counsellors at Law

Contents

1. Digital Economy p.5
1.1 Key Challenges p.5
1.2 Digital Economy Taxation p.7
1.3 Taxation of Digital Advertising p.8
1.4 Consumer Protection p.8
1.5 The Role of Blockchain in the Digital Economy p.9

2. Cloud and Edge Computing p.9
2.1 Highly Regulated Industries and Data Protection p.9

3. Artificial Intelligence p.10
3.1 Liability, Data Protection, IP and Fundamental Rights p.10

4. Internet of Things p.12
4.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection p.12
4.2 Compliance and Governance p.13
4.3 Data Sharing p.13

5. Audiovisual Media Services p.14
5.1 Requirements and Authorisation Procedures p.14

6. Telecommunications p.15
6.1 Scope of Regulation and Pre-Marketing Requirements p.15
6.2 Net Neutrality Regulations p.17
6.3 Emerging Technologies p.17

7. Challenges with Technology Agreements p.18
7.1 Legal Framework Challenges p.18
7.2 Service Agreements and Interconnection Agreements p.19

8. Trust Services and Digital Entities p.19
8.1 Trust Services and Electronic Signatures/Digital Identity Schemes p.19

9. Gaming Industry p.20
9.1 Regulations p.20
9.2 Regulatory Bodies p.21
9.3 Intellectual Property p.21

10. Social Media p.22
10.1 Laws and Regulations for Social Media p.22
10.2 Regulatory and Compliance Issues p.23

Contributed by: Agus Ahadi Deradjat (Agung), Mahiswara Timur, Nina Cornelia Santoso and Natasya Nurul Amalia, **ABNR Counsellors at Law**

ABNR Counsellors at Law was founded in 1967 and is Indonesia's longest-established law firm. ABNR pioneered the development of international commercial law in the country following the reopening of its economy to foreign investment after a period of isolationism in the early 1960s. With more than 100 partners and lawyers (including three foreign counsel), ABNR is the largest independent full-service law firm in Indonesia and one of the country's top three law firms by number of fee earners, giving it the scale needed to simultaneously handle large and complex transnational deals across a range of practice areas. The firm also has global reach as the exclusive Lex Mundi member firm for Indonesia since 1991. Lex Mundi is the world's leading network of independent law firms, with members in more than 100 countries.

Authors

Agus Ahadi Deradjat (Agung) is a partner at ABNR Counsellors at Law and a former member of the firm's management board. Agung focuses his practice on corporate/M&A, foreign direct investment (FDI) and TMT. He advises leading domestic and multinational corporations across all major industries and sectors, but offers particular expertise and experience in life sciences, technology and telecommunications, e-commerce and automotive. Agung recently worked on a number of major M&A and FDI transactions for high-end multinational clients, as well as significant FDI transactions in the technology, pharma, manufacturing, chemicals and natural resources sectors. Agung is ranked for TMT (Band 1) and corporate/M&A by Chambers Asia-Pacific.

Mahiswara Timur joined ABNR Counsellors at Law as an associate in June 2015 and became a senior associate in January 2021. Timur has focused on IT-related assignments such as telecommunications networks (including for submarine cables and satellites) and services, cybersecurity, personal data protection, content compliance, cloud computing, e-commerce, broadcasting, over-the-top services, data centre and digital platform services, the IoT and online games. He has advised start-up clients and leading multinational technology, social media and streaming companies. His extensive understanding of the regulatory, technical and practical aspects of TMT business has enabled Timur to provide precise, comprehensive advice and practical solutions well-tailored to client needs and business operations.

Contributed by: Agus Ahadi Deradjat (Agung), Mahiswara Timur, Nina Cornelia Santoso and Natasya Nurul Amalia, **ABNR Counsellors at Law**

Nina Cornelia Santoso joined ABNR in April 2015 and became a senior associate in January 2022. Nina's main areas of professional practice encompass technology, media and telecommunications (TMT), competition, mergers and acquisitions (M&A) and foreign direct investment (FDI). Concerning TMT, she regularly advises high-profile multinational and local companies on privacy and data protection, internet-based products and services (digital platforms, social media, online games, cloud computing, e-commerce, over-the top services), cybersecurity and content moderation. She occasionally advises clients on telecommunications network and service matters (including subsea cables). Her graduate studies at the University of Cambridge also contributed to her profound knowledge of the EU General Data Protection Regulation (GDPR).

Natasya Nurul Amalia joined ABNR in April 2015 and focuses her professional practice on technology, media and telecommunications (TMT). Her TMT work includes data privacy and protection, e-commerce, digital content compliance, cybersecurity, advertising, online gaming and general advice on technology services and compliance in Indonesia. She is also familiar with fintech industry agreements and has advised on the compliance of fintech business models with Indonesian regulations. In 2022, she earned an LLM degree from the University of California, Berkeley, with a certificate of specialisation in law and technology.

ABNR Counsellors at Law

Graha CIMB Niaga 24th Floor
Jl. Jenderal Sudirman Kav 58
Jakarta 12190
Indonesia

Tel: +62 21 250 5125/5136
Fax: +62 21 250 5001
Email: info@abnrlaw.com
Web: www.abnrlaw.com

Contributed by: Agus Ahadi Deradjat (Agung), Mahiswara Timur, Nina Cornelia Santoso and Natasya Nurul Amalia, ABNR Counsellors at Law

1. Digital Economy

1.1 Key Challenges

As in other parts of the world, the digital economy plays a pivotal role in shaping Indonesia, particularly as a developing country that is heavily reliant on various types of inbound investment. The Indonesian government has been quite aggressive in introducing new regulations (or, in some cases, updates to current regulatory regimes) in order to accommodate digital economy-related trends.

The government has made efforts to regulate the digital economy and understands the dynamics of, and rapid changes in, the digital economy. The government is using both regulations, as "hard law", and policies to govern this sector. This approach has been taken to allow the government to balance the mandatory legal requirements with the implementation of additional requirements that might be necessary for dealing with new business models or issues. However, this approach may lead to inconsistent enforcement and uncertainties for industry players from time to time.

The Indonesian digital economy is mainly regulated under the following laws and regulations.

General Operation of Electronic Systems

The advancement of the digital economy is inseparable from the widespread use of electronic systems. The operation of electronic systems in Indonesia is regulated under the following laws and regulations:

- Law No 11 of 2008 as last amended by Law No 1 of 2024 on Electronic Information and Transactions (the "EIT Law");
- Government Regulation No 71 of 2019 on the Provision of Electronic Systems and Transactions (GR 71);
- Minister of Communications and Information Technology (the MCIT, currently known as the Minister of Communications and Digital or the MOCD) Regulation No 20 of 2016 on Personal Data Protection in Electronic Systems (MR 20); and
- MOCD Regulation No 5 of 2020 on Private Electronic Systems Operators, as amended by MOCD Regulation No 10 of 2021 (MR 5).

An electronic system operator (ESO) would be subject to these obligations:

- obtaining an ESO registration certificate – the operator of an electronic system must register themselves with the MOCD if they provide their digital platforms within the Indonesian territory or carry out business in Indonesia, or if their electronic systems are used or offered within Indonesian territory;
- applying content moderation – the ESO must ensure that its electronic system does not contain prohibited electronic information and/or electronic documents and does not facilitate the distribution of prohibited electronic information and/or electronic documents (eg, pertaining to pornography, gambling, slander, scam, hate speech, violence, intellectual property (IP) rights infringement, information security breach, content that causes public disturbance, content that violates social norms, hoax/fake news or extortion);
- using secure and compatible hardware and secure and reliable software;
- maintaining security measures for the components of electronic systems; and
- complying with the minimum requirements for the operation of electronic systems stipulated under the regulations.

E-Commerce

Government Regulation No 80 of 2019 on E-Commerce (GR 80) serves as the umbrella law for e-commerce transactions. GR 80 governs the main aspects of e-commerce, including licensing requirements, obligations for e-commerce providers, content liability, consumer protection and data protection.

GR 80 generally defines "e-commerce" as a form of commerce in which transactions are conducted using electronic equipment and procedures, whereas an "e-commerce undertaking" is "an individual or undertaking, whether incorporated or unincorporated and whether domestic or non-domestic, that engages in commercial operations in the e-commerce field". Considering the broad definition of e-commerce, many electronic platforms would qualify as an e-commerce undertaking and should comply with e-commerce regulations' provisions.

E-commerce undertakings are further classified into three categories:

- e-commerce providers – providers of electronic communication facilities used for trading transactions;
- merchants – business undertakings engaged in e-commerce, either by using e-commerce facilities created and managed directly by themselves or through a facility owned by an e-commerce provider (or through other electronic systems that provide an e-facilities platform); and
- intermediary service providers (ISPs) – domestic or foreign business actors (other than telecommunications operators) that provide an electronic communications platform, which only functions as an intermediary in electronic communications between a sender and recipient.

E-commerce undertakings are required to obtain the relevant licences via the online single submission system.

The Ministry of Trade (MOT) also issued Regulation No 31 of 2023 on Licensing, Advertising, Development and Supervision of Business Undertakings in the E-Commerce Sector (MR 31) as an amendment to the previous implementing regulation of GR 80.

Notable provisions governing the obligations of e-commerce undertakings under GR 80 and MR 31 include the following.

- Content moderation - e-commerce providers shall be held liable for the legal consequences/impact of illegal electronic information/content on their platform. However, GR 80 provides a safe harbour if the e-commerce provider takes immediate action to delete a link to illegal electronic content once aware of its nature.
- Product compliance for foreign merchants – foreign merchants are required to verify their identity and provide specified documentation and information to an e-commerce provider, including:
  - (i) identity details;
  - (ii) a copy of a business licence that has been apostilled by an authorised institution or legalised by an Indonesian embassy overseas;
  - (iii) evidence of compliance with the relevant compulsory standards and technical requirements for the goods/services being sold;
  - (iv) bank account numbers used for transaction payments; and
  - (v) a certificate or report confirming the veracity of the merchant's identity particulars and business licence from an

independent surveyor in the merchant's country of origin.

MR 31 tries to capture platforms that provide both social media and e-commerce within the same application by introducing the term "social commerce", which is defined as a "social media operator that provides certain features, menus or facilities that enable merchants to offer goods or services". Social commerce platforms are also prohibited from acting as a manufacturer and facilitating payment transactions.

MR 31 also provides for specific business models that are subject to the e-commerce regulations - namely online retail, online marketplaces, online classified advertising, price comparison platforms and daily deals.

Payment Service Providers

The payment system industry is also a major contributor to the growth of Indonesia's digital economy. However, this industry is considered a highly regulated sector under the authority of Indonesia's central bank, Bank Indonesia (BI). The two regulatory frameworks regulating payment services activities are BI Regulation No 22/23/PBI/2020 on Payment Systems and BI Regulation No 23/6/PBI/2021 on Payment Service Providers (PBI 23).

Under PBI 23, the main activities of payment service providers (PSPs) include account issuance services, account information services, payment initiation and/or acquiring services and money remittance services. PSPs may be required to obtain different licences depending on the types of business activities they provide, which are categorised into three types under PBI 23:

- category 1 - account issuance services, account information services, payment initiation and/or acquiring services and money remittance services (eg, issuer);
- category 2 – account information services and payment initiation and/or acquiring services (eg, acquirer, payment gateway provider, e-wallet provider); and
- category 3 - money remittance services and/or other services determined by BI.

The categorisation is designated to compartmentalise various types of payments services, according to their degree of involvement in payment processing and attributed risks. A business model with inherently greater risk would be subject to higher scrutiny and licensing requirements.

The ever-evolving digital payment ecosystem poses a practical challenge. Business undertakings often find it quite difficult to determine the appropriate licences under PBI 23 for their business models.

1.2 Digital Economy Taxation

Digital services and goods in Indonesia are subject to Ministry of Finance Regulation No 81 of 2024 on the Tax Provisions in the Framework of Implementing the Core Tax Administration System (MOFR 81). Any utilisation of foreign digital goods and digital services within the territory of Indonesia via e-commerce shall be subjected to value added tax (VAT). The VAT rate is 11% per transaction and is imposed on foreign merchants and/or foreign service providers. As per 1 January 2024, delivered or imported luxury goods (which are subject to the Sales Tax on Luxury Goods) are subject to VAT of 12% of the selling price or import price.

Digital goods and services covered under MOFR 81 include the following.

- Digital goods: any intangible goods, in the form of electronic or digital information, resulting from conversion or that were originally in electronic form, such as software, multimedia and/or electronic data. Digital goods include electronic games, e-books, music, etc.
- Digital services: any services sent via the internet or electronic networks that can only be used via IT, including but not limited to software-based services. Digital services include online advertising, online consultation, digital marketing, etc.

1.3 Taxation of Digital Advertising

As "digital services" under MOFR 81 also covers digital advertising, digital advertising that originates from foreign service providers is subject to the 11% VAT rate (projected to increase to 12%).

1.4 Consumer Protection

Law No 8 of 1999 on Consumer Protection (the "Consumer Protection Law") serves as the umbrella regulation for safeguarding consumer rights. The Consumer Protection Law generally applies to all types of goods and services, including those in the digital realm. In addition, specific provisions on consumer protection under GR 71 and MR 31 are also applicable to digital goods and services in the TMT sector.

To ensure compliance with the Consumer Protection Law, undertakings that operate in the digital economy and offer digital goods and services must, among other things:

- not offer, promote or advertise goods and services deceivingly;
- not make false or misleading advertisements or claims;
- not directly or indirectly degrade other goods and/or services;
- provide a refund mechanism for consumers who wish to cancel their purchases; and
- provide a time limit for consumers to return the sent goods and/or delivered services, should there be any discrepancy with the contract or hidden defect.

Consumer Complaint Service

GR 80 requires e-commerce business undertakings to protect consumers' rights in accordance with the consumer protection regulations, including the Consumer Protection Law and any sector-specific regulations that may be applicable for such undertakings (eg, consumer protection provisions on payment instruments that are governed under the payment system regime).

MR 31 further stipulates that e-commerce operators must provide a consumer complaint service, which must be visible to all customers accessing the products and display (i) the e-commerce operator's contact information for consumer's complaints and (ii) the Directorate General of Consumer Protection of Ministry of Trade's contact information.

Dispute Resolution Forum for Consumer-Related Disputes

Theoretically, the Consumer Protection Law ensures the right of consumers to file a lawsuit against business undertakings via an in-court or out-of-court dispute settlement, depending on the choice of forum agreed by the disputing parties. However, the latest EIT Law amendment requires parties to an international electronic transaction that contains standardised clauses made by an ESO to be governed by Indonesian law, in the event that the contract involves an Indonesian party or is implemented in Indonesia.

To handle consumer disputes effectively, it is best practice for companies offering digital ser-

vices and products to provide a dedicated channel and detailed guidelines on the complaint management process.

1.5 The Role of Blockchain in the Digital Economy

Ever since its existence was recognised by the Indonesian government in 2020, cryptocurrency, which is based on blockchain technology, has massively transformed the Indonesian digital economy landscape.

Following the enactment of Law No 4 of 2023 on the Development and Reinforcement of the Financial Sector, the management of cryptocurrency was to be effectively transferred from the Indonesian Commodity Futures Trading Regulatory Agency (*Bappebti*) to the Financial Services Authority (*Otoritas Jasa Keuangan*; OJK) by January 2025 at the latest. This change was aimed at harmonising cryptocurrency with other forms of financial services regulated under the OJK. However, this concrete change in authority is dependent upon a government regulation, which is yet to be issued.

In 2024 alone, the cryptocurrency transaction value exceeded IDR500 trillion according to *Bappebti* . Despite the immense size of the market, cryptocurrency is a commodity that can only be traded on a specific platform, called the Crypto Asset Physical Market, and it is not recognised as a valid instrument of payment under the Currency Law. The government is continuously making efforts to ensure that cryptocurrency remains as a commodity, and cannot be used as a payment instrument, by comprehensively regulating the flow of transactions that could be made by crypto-asset-related business undertakings as well as by expressly prohibiting PSPs from concluding or processing any payment in cryptocurrency.

2. Cloud and Edge Computing

2.1 Highly Regulated Industries and Data Protection

It is a universal value that efficiency is key for doing business, which leads to the adoption of cloud services as a means to scale up digital infrastructure with minimum expense. Cloud and edge computing increase the accessibility of advanced technology.

In Indonesia, cloud and edge computing have not been regulated yet. However, some general compliance related to the EIT Law, Law No 27 of 2022 on Personal Data Protection (the "PDP Law") and the Consumer Protection Law is applicable to the use of cloud computing, with greater restrictions applying to certain industries such as the financial sector and healthcare.

Financial Sector

Banks are generally allowed to co-operate with third-party IT providers in implementing their IT (including the use of cloud computing). However, the co-operation must comply with the requirements under OJK Regulation No 11/POJK.03/2022 on Implementation of Information Technology by Commercial Bank (POJK 11), such as:

- having supervision over the implementation of the third-party provider services;
- the procurement of the third-party provider must consider the matters provided under POJK 11; and
- having a co-operation agreement with minimum provisions, as set out in POJK 11.

If a bank intends to co-operate with a foreign IT service provider for any IT-based transaction processing, it must obtain approval from the OJK. The regulation also requires banks to

locate their data centres and/or disaster recovery centres in Indonesia, unless otherwise approved by the OJK.

Similarly, non-bank financial institutions are also subject to data localisation requirements under OJK Regulation No 4/POJK.05/2021 on the Implementation of Risk Management in Using Information Technology by Non-Bank Financial Services Institutions, as partially revoked by OJK Regulation No 10/POJK.05/2022 on Peer-to-Peer Lending (POJK 4).

Healthcare

Under Ministry of Health (MOH) Regulation No 24 of 2022 on Medical Records, medical records can be stored on digital-based storage media at health service facilities, including on servers, via certified cloud computing and via any other certified digital-based storage media. Healthcare facilities can co-operate with an ESO that has onshore data storage facilities that have been white-listed by the MOH.

Processing of Personal Data in the Context of Cloud Computing

In many instances, cloud computing services would be procured from a third-party provider. In such case, the third-party provider must confirm their role in the personal data processing (eg, whether they act as the data processor of the data controller). This is crucial for the third-party cloud computing provider, as the PDP Law differentiates between the liability of a data controller and data processor. Thus, the third-party cloud computing provider and the user should establish a set of clear provisions on the role, obligations and liability of each party in the context of personal data processing.

In addition, the adoption of cloud computing technology may pose greater security risks to users' personal data as the technology may be more susceptible to cyber-attack, particularly if the solution is deployed without using a private network. Thus, business undertakings must ensure that cloud computing service providers are offering adequate robust security measures to mitigate those vulnerabilities, which shall be proportionate with the potential risk.

3. Artificial Intelligence

3.1 Liability, Data Protection, IP and Fundamental Rights

Artificial intelligence (AI) has also reached Indonesia. The popularity of generative AI (eg, ChatGPT) has led to a rapid increase in its usage and integration in a variety of sectors. This has resulted in concerns about compliance, as Indonesian regulations do not yet specifically encompass this particular technology, rather relying on existing general regulations.

As a response to the rapid utilisation of AI, the MCIT issued Circular Letter No 9 of 2023 on Ethics of Artificial Intelligence (CL 9). CL 9 is essentially a guideline, which is focused more on supervision and governance in order to reduce potential risks. CL 9 is intended as a pointer to ethical values for business actors that use AI-based software.

The scope of CL 9 includes general definitions and guidelines pertaining to values, ethics, consulting, analysis and programming activities, with an AI basis, for business actors and electronic systems operators.

Ethical values of AI introduced under CL 9 include – among others - inclusivity, humanity, safety, accessibility, transparency, credibility, accountability, personal data protection, sus-

tainable development, the environment and IP rights.

There are three ways for business actors, public ESOs and private ESOs to honour their ethical responsibilities when it comes to AI, namely by:

- ensuring AI is not implemented as a policy-maker and/or decision-maker with implications for humanity;
- providing information about the development of AI-based technology by developers to prevent negative impacts and losses resulting from the technology; and
- taking into account risk management and crisis management in AI development.

In addition to the CL 9, the OJK has introduced the Code of Ethics for Responsible and Trustworthy AI in the Financial Technology Industry (the "OJK Code of Ethics"). According to the basic principles enshrined under the OJK Code of Ethics, among other things, AI should be:

- based on *Pancasila* (the official, foundational philosophical theory of Indonesia);
- beneficial;
- fair and accountable;
- transparent and explicable; and
- robust and secure.

The current government's approach allows for flexibility in the development of AI-based technology in Indonesia, while also allowing for a "wait and see" approach to determining the appropriate measures to govern this technology.

Measures in Relation to Deepfake Technologies

Deepfake technologies serve as a prime example of a "double-edged sword" emerging from the development of AI. Regulation that can be applied to mitigate the downsides of this technology includes the following.

Copyright law

When an original work is altered using deepfake technology, it may infringe provisions under copyright law, particularly concerning unauthorised modifications or derivative works. This may harm the original creator's exclusive rights, namely their:

- economic rights – ie, the right to derive economic benefits from a creation, including to reproduce the creation in any form, adapt, arrange or transform it, distribute it – or copies thereof – and display it; and
- moral rights, including the right to prevent distortion, modification, mutilation or other actions that harm the honour or reputation of the creator, unless such actions are approved.

Accordingly, the copyright owner/holder may exercise their rights to prohibit the illegal reproduction, adaptation or transformation of content created using deepfake technology, as a measure to protect their economic and moral rights.

In addition to criminal measures, the creator or copyright holder may pursue legal action against individuals who intentionally, without proper authorisation or consent, infringe upon the performer's moral rights, including seeking compensation for damages.

The EIT Law

Under the EIT Law, the creation and use of deepfake technologies may also entail several legal risks, as stipulated in:

- Article 28 (1), which prohibits the dissemination of false information that causes material damages to the consumer;

- Article 28 (3), which prohibits the dissemination of false information capable of inciting public unrest; and
- Article 35, which prohibits the manipulation or creation of electronic information to falsely appear authentic.

As stipulated under the EIT Law, any violation of Article 28 (1) or (3) may be subject to criminal sanction, namely imprisonment for up to six years and/or a fine of up to IDR1 billion. Further, violation to Article 35 of the EIT Law is subject to imprisonment for up to 12 years and/or a fine of up to IDR12 billion.

4. Internet of Things

4.1 Machine-to-Machine Communications, Communications Secrecy and Data Protection

Internet of things (IoT) applications continue to rapidly evolve in this increasingly technology-reliant era. From smart homes that optimise energy consumption to industrial applications that streamline production processes, the IoT offers substantial scope for transformation and increased operational efficiency.

In Indonesia, while not yet being specifically regulated in detail, the IoT is starting to be acknowledged, as indicated by the inclusion of KBLI 62024 – IoT Consultation and Design Activities as an Indonesian standard business classification, which encompasses consulting services and designing and manufacturing integrated system solutions based on orders (not "ready to use") by modifying existing hardware, such as sensors, micro-controllers and other hardware and/or embedded software.

Furthermore, acknowledgement of the IoT is reflected in the incorporation of several International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) IoT standards into the Indonesia National Standard by the Ministry of Industry pertaining to:

- technical requirements for the application of sensor networks for wireless gas meters;
- IT – internet-based use of IoT systems;
- reference architecture;
- the interoperability of IoT systems;
- vocabulary; and
- sensor network testing frameworks.

In addition to the foregoing, elements that could be relevant to the operation of IoT applications have been included in several laws and regulations, as follows.

Provision of IoT Services Under the Telecommunications Regime

The provision of IoT services heavily relies on stable and adequate telecommunications connectivity, as one of the main elements of IoT services. MR 5 stipulates that the provider of IoT services must either:

- obtain a business licence for the operation of the telecommunications services (*Perizinan Berusaha Penyelenggaraan Jasa Telekomunikasi*) of a data communication system from the MOCD; or
- co-operate with the telecommunications provider of a data communications system.

Connectivity providers are also required to implement a unique addressing system, including (but not limited to):

- a local Mobile Station Integrated Services Digital Network (MSISDN);

- device end-user IDs; or
- internet protocol numbers.

Electronic Agents

Although not specifically regulated, the automatisation of information processing possible with the IoT render it comparable to an "electronic agent" under Indonesian law. The EIT Law essentially defines an electronic agent as "a device of an electronic system that is made to perform an action based on certain electronic information provided automatically by a person". The phrase "automatically by a person" refers to natural persons or legal entities (both Indonesian citizens and foreign nationals).

Data Protection

All personal data processing activities involved in the operation of the IoT will fall within the material scope of the PDP Law, given that IoT devices may process personal data. The key data protection challenges relevant to the use of the IoT are as follows.

Difficulty in determining responsibility upon failure to protect personal data

IoT services typically involve more parties than mobile operators. Given the multitude of components involved, it is essential to conduct an assessment of data processing activities in order to determine the relevant data protection roles (ie, data controller or data processor) and their attendant obligations.

Abuse of data collection

Private entities that provide IoT devices or services that can access IoT data may use or disclose personal information for additional purposes, such as profiling, targeted advertising or the sale of data to data brokers. In accordance with the PDP Law, the data controller must secure the appropriate lawful basis for data processing and inform the data subject in a transparent manner.

4.2 Compliance and Governance

The deployment of the IoT in Indonesia offers numerous opportunities across various sectors. However, it also introduces significant challenges for companies offering IoT services in terms of compliance and governance. These companies must navigate IoT-related regulations, including fulfilling the mandatory certification requirements outlined in MOCD Regulation No 3 of 2024 on Standardization and Certification of Telecommunication Equipment. The certification process requires device importers, manufacturers, distributors and brand owners/licensees to ensure that their devices are compliant with the relevant technical standards determined for each type of device and technology.

4.3 Data Sharing

IoT companies might be subject to (i) personal data protection regulations (ie, the PDP Law and its implementing regulations) if sharing personal data and (ii) sector-specific regulations if data sharing would involve specific industries (eg, financial institutions).

Cross-Border Personal Data Transfer Requirements

Cross-border personal data transfer by a data controller may only be performed upon meeting the following conditions under the PDP Law, which must be assessed and implemented in sequence:

- adequacy of protection – the country of domicile of the receiving data processor and/or data controller has a personal data protection level that is equal or higher than the PDP Law;

- appropriate safeguard – adequate and binding personal data protection is in place – whilst the PDP Law is silent on what would constitute an appropriate safeguard, it is possible that a contractual instrument or binding rules would be sufficient, subject to a future implementing regulation; and
- consent from data subjects.

Sharing of Specific Categories of Data

The processing of specific categories of personal data (including data pertaining to health, biometrics, genetics, criminal records, children, etc, as specified under the regulations) is subject to heightened requirements to carry out a data protection impact assessment.

Requirements for Specific Industries

The following industries are subject to sector-specific requirements with respect to the sharing of data.

- Financial services: It is a requirement that potential consumers provide consent for data/information sharing as a prerequisite to using a financial institution's products and/or services; and
- Healthcare: Law No 17 of 2023 on Health generally protects the confidentiality of personal health data and information, unless waived at the patient's request. Specifically, Minister of Health Regulation No 24 of 2022 on Medical Records allows the disclosure of medical records at the request of the patient.

5. Audiovisual Media Services

5.1 Requirements and Authorisation Procedures

The regulatory frameworks applicable to audiovisual media services and video-sharing platform services in Indonesia depend on whether they are broadcasting companies or internet-based video-sharing platforms.

Broadcasting Companies

Broadcasting companies are generally subject to Law No 32 of 2022 on Broadcasting as amended by Law No 6 of 2023 on Ratification of Government Regulation in Lieu of Law No 2 of 2022 on Job Creation as a Law (the Broadcasting Law) and its implementing regulations. The Broadcasting Law applies to the activity of broadcasting through transmitting facilities with or without use of the radio frequency spectrum; this covers radio and television broadcasts and excludes over-the-top (OTT) streaming services.

Prior to conducting broadcasting activities, broadcasting companies must obtain a broadcasting operation licence (*izin penyelenggaraan penyiaran*) from the MOCD.

Aside from the Broadcasting Law, broadcasting companies must also comply with the content-related provisions under Law No 33 of 2009 on Film, as amended by Law No 11 of 2020 on Job Creation (eg, on censorship), as well as with the EIT Law (eg, on the distribution or transmission of prohibited electronic information/electronic documents).

Internet-Based Video-Sharing Platforms

The Constitutional Court has clearly established that internet-based video-sharing platforms are beyond the scope of the Broadcasting Law. Thus, business undertakings that provide video-sharing platform services are deemed ESOs under the supervision of the MOCD and hence are subject to the laws and regulations on electronic systems. The providers of internet-based video-sharing platforms must comply with the obligations of an ESO, including the mandatory

requirement to obtain an ESO registration certificate as well as an e-commerce business licence.

Takedown Requests

One of the most substantial issues related to video-sharing platforms concerns content compliance.

According to MR 5, GR 71 and the EIT Law, platform operators must ensure that their platforms do not contain or facilitate the distribution of prohibited content and comply with takedown requests (TDRs) issued by the MOCD.

The MOCD tries to establish strict compliance by platform operators through establishing a mechanism that allows the MOCD to impose a monetary fine for non-compliance with TDRs, which is calculated based on a certain formula and variables including the business scale, type of content, severity of the violation, compliance level, etc.

6. Telecommunications

6.1 Scope of Regulation and Pre-Marketing Requirements

Telecommunications is a highly regulated industry in Indonesia and is under strict supervision by the MOCD. The Indonesian government differentiates between (i) telecommunications networks and (ii) telecommunications services. Further, as a response to the emergence of alternatives to telecommunications services, the MOCD has been increasing their focus on regulating OTT service providers.

The government has also recognised several new technologies including the 5G network, which promises faster and more reliable internet connectivity, and Starlink.

The telecommunications industry is governed under the following regulations:

- Law No 36 of 1999 on Telecommunications as amended by Law No 6 of 2023 on Job Creation (the "Telco Law");
- Government Regulation No 52 of 2000 on the Operation of Telecommunications, partially revoked by Government Regulation No 46 of 2021 on Posts, Telecommunications and Broadcasting;
- MCIT Regulation No 01/PER/M.KOMINFO/01/2010 on the Operation of Telecommunications Networks, amended several times, most recently by MCIT Regulation No 5 of 2021 on the Operation of Telecommunications;
- MCIT Regulation No 12 of 2018 on Provision of Special Telecommunications for the Needs of Government Agencies or Legal Entities;
- MCIT Regulation No 13 of 2019 on the Operation of Telecommunications Services, amended several times, last by MCIT Regulation No 14 of 2021;
- MCIT Regulation No 5 of 2021 on the Operation of Telecommunications (MR 5/2021); and
- Government Regulation No 46 of 2021 on Posts, Telecommunications and Broadcasting (GR 46/2021).

Pursuant to the Telco Law, telecommunication is defined as "the transmission, delivery, and/or receipt of information in the form of signs, signals, text, images, sounds, or noises through wire, optical, radio, or other electromagnetic systems".

Although the telecommunication industry is subject to stringent regulations, the existing legislation does not lay out specific security requirements.

Telecommunications Services

Under the Telco Law, telecommunications services are classified as follows:

- telecommunications network – a network that enables the implementation of telecommunications – this covers the provision of fixed network and mobile network operations (cellular, satellite or terrestrial);
- telecommunications services – services that enable the implementation of telecommunications – this covers basic telephony service providers, value-added telephony service providers, multimedia services (ISPs, network access points (NAPs), data communication services and internet protocol television services); and
- special telecommunications services – telecommunications operations that are specialised in nature, designation and operation (ie, designed for research or government agencies).

The operation of telecommunications in Indonesia may only be performed by a licensed Indonesian legal entity.

Radio Frequency Spectrum Use

The radio frequency spectrum is considered a finite resource in Indonesia. Its use in telecommunications services is therefore regulated under MCIT Regulation No 7 of 2021 on the Use of Radio Frequency Spectrum, as partially revoked by MCIT Regulation No 9 of 2023 (MR 7), which distinguishes three licences that must be obtained by businesses:

- radio frequency band licence (*Izin Pita Frekuensi Radio* IPFR) - a licence to use the radio frequency spectrum in the form of a radio frequency band;
- radio station licence (*Izin Stasium Radio* ISR) - a licence to use the radio frequency spectrum in the form of a radio frequency channel; and
- class licence - a licence for the use of the radio frequency spectrum in association with a telecommunications tool and/or telecommunications equipment certificate.

Further, in an effort to boost the development of telecommunications technology in Indonesia, the government allows a spectrum-sharing arrangement, which is subject to contractual agreement between telecommunications operators.

Certification of Telecommunications Equipment and/or Devices

Pursuant to MCIT Regulation No 16 of 2018 on Operational Provisions for the Certification of Telecommunications Equipment and/or Devices, telecommunications devices manufactured, assembled or imported to be traded and/or used in Indonesia must be certified to prove they are compliant with the prescribed technical specification and/or standards.

Internet Business Undertaking

GR 46/2021 refers to OTT services as business activities conducted via the internet in the form of telecommunications service substitutes, audio and/or visual content platforms and/or other services as determined by the MOCD.

OTT services providers must co-operate with local telecommunications operators, pursuant to MR 5/2021, upon meeting a “significant presence” criterion based on the traffic percentage or daily active user volume.

Although the regulations do not provide sanctions for non-compliance with the co-operation requirement, GR 46/2021 and MR 5/2021

authorise telecommunications operators to enforce traffic management, which could be broadly interpreted to include bandwidth throttling.

Recent Updates on the Telecommunications Industry

5G Network

In July 2024, the MOCD issued Decree No 352 of 2024 on the Technical Standards for Telecommunications Equipment and/or Mobile Telecommunications Devices Based on Long Term Evolution Technology Standards and International Mobile Telecommunications Technology Standards-2020 (MD 352), which stipulates that the 5G bandwidth for SS 5G NR FR1 Stand Alone is n28, whereas that for SS 5G NR FR2 Stand Alone is n258.

Starlink

As of April 2024, Starlink has provided internet services to several rural communities in Indonesia using low Earth orbit satellites. This technology provides a competitive advantage over other conventional ISPs in Indonesia.

Pursuant to MR 13/2019, any ISPs operating in Indonesia must establish a physical presence and build their own network operation centre (NOC) in Indonesia. If foreign ISPs do not fulfil these requirements, they are required to co-operate with Indonesian ISPs via a NAP.

As of this writing, the government is aiming to limit Starlink's activity to rural areas only, which cannot be covered by existing ISPs.

6.2 Net Neutrality Regulations

Net neutrality regulations can be understood as the government's effort to protect consumers' rights by preventing ISPs from blocking or degrading the service of its competitors. Currently, Indonesia does not have net neutrality regulations in place, meaning there are no limitations on ISPs with respect to blocking or preventing their consumers from accessing competitors' services. However, general competition law provisions apply.

It should be noted that MR 5/2021 requires certain business undertakings that meet significant criteria to co-operate with local licensed telecommunications operators. These business undertakings include:

- telecommunications service substitutes;
- OTT service operators; and
- broadcasting service substitutes and other services determined by the MOCD.

It is essential that such co-operation adheres to the principles of fairness, equity and non-discrimination, while also ensuring consistent quality of services as stipulated by the relevant laws and regulations. In the absence of such co-operation, the telecommunications operator has the right to implement traffic management measures.

6.3 Emerging Technologies

The telecommunications industry in Indonesia is heavily regulated, with telecommunication service providers having to fulfil several requirements before being able to operate. This means that emerging technologies such as the IoT and AI will most likely have little-to-no impact on the nation's telecommunication industries, as such technologies do not alleviate the strict requirements that telecommunication providers are subject to.

However, emerging technologies that rely heavily on infrastructures like 5G technology are more likely to be regulated by the government. In such

case, the government issued MD 352, which regulates the bandwidth that 5G networks can operate on. In contrast, Starlink's direct-to-cell technology, which provides direct internet service from its satellites to the user's cell phone, is still under the government's watch.

7. Challenges with Technology Agreements

7.1 Legal Framework Challenges

In the ever-evolving tech industry, numerous business models are emerging that have not yet been addressed by current laws and regulations. As a result, a thorough evaluation is essential to ensure these new models are both legal and compatible with existing regulatory frameworks.

In navigating this complex landscape, it is imperative to carefully weigh the need for sovereignty with the need to facilitate technological advancement. The Indonesian government has attempted to do so by allowing freedom of use of foreign data centres as stipulated in GR 71, provided that there is a guarantee of data accessibility to facilitate supervision and law enforcement.

When entering into a technology agreement with a local organisation, the "freedom of contract" principle applies. However, should a technology agreement encompass certain industries, such as the financial and health sectors, they may be subject to greater restrictions.

Recommended Clauses in Technology Agreements

Data protection clauses

Data protection clauses in technology agreements act as a critical safeguard for parties involved in the agreement, ensuring that personal and sensitive data is handled with care and in compliance with relevant laws and regulations.

Data protection clauses include clauses on the roles of each party in the processing of personal data, cross-border data transfer requirements and data subjects' rights.

Local language clause

Pursuant to Law No 24 of 2009 on National Flag, Language, Coat of Arms, and Anthem, any agreements involving an Indonesian individual or legal entity must include the Indonesian language.

Therefore, any agreements that are designed for Indonesian consumers must at least be accompanied by a separate version exclusively drafted in the Indonesian language (bilingual language is acceptable).

Restrictions Under EIT Law

As noted in **1.4 Consumer Protection** , parties to an international electronic transaction that contains standardised clauses made by an ESO must be governed by Indonesian law.

Restrictions for Financial and Health Sectors

There are greater restrictions and obligations in relation to data localisation for the financial and health sectors, which mandate data localisation. Exemption may apply upon obtaining approval from a regulator such as the OJK or MOH (as applicable).

Financial institutions may require OJK or BI approval prior to entering into agreements with third-party technology providers.

7.2 Service Agreements and Interconnection Agreements

MR 5/2021 requires telecommunications operators to comply with a minimum service level agreement based on the quality standard set by the MOCD. Parties may refer to the following regulations issued by the MOCD in drafting telecommunications agreements:

- Directorate General of Post and Information Services Regulation (DGPR) No 1 of 2021, as amended by DGPR No 1 of 2023, on the Technical Provisions on the Implementation of Telecommunications Services; and
- DGPR No 7 of 2024 on Implementation of Telecommunication Network Quality Standard.

Interconnection Agreements

MR 5/2021 conceives of interconnection as the connectivity between telecommunication networks from different network providers. For interconnection to occur, the different network providers need to execute an interconnection agreement.

The main interconnection agreement encompasses, among other elements, service quality and scope, capacity and forecasting, the provision of information and confidentiality, calling line identification, the interconnection of services from providers, the issue of fraud, fees, billing and payment. The agreement must also be supported by documents pertaining to planning and operation, billing and payments, a list of interconnection services, technical specifications and definitions and interpretations.

Interconnection prices are determined on a cost basis by considering the economic value and are subject to the standard formulation provided by the government. Concerning tariffs, the MOCD has the authority to determine the recommended minimum and/or maximum tariff.

8. Trust Services and Digital Entities

8.1 Trust Services and Electronic Signatures/Digital Identity Schemes

Trust Services

Under Indonesian laws and regulations, trust services are managed by certification authorities. The EIT Law stipulates that a certification authority may provide the following:

- electronic signatures (e-signatures);
- an electronic seal;
- electronic time stamps;
- a registered electronic delivery service;
- website authentication;
- preservation of electronic signatures and electronic seals;
- a digital identity; and
- other services that use electronic certificates.

The EIT Law and MCIT Regulation No 11 of 2022 on Implementation of Electronic Certification Governance require certification authorities offering electronic certification and providing services that use electronic certificates in Indonesia to be Indonesian legal entities domiciled in Indonesia, except where the services are not available in Indonesia. Although this requirement is mainly intended to promote local certification authorities, this raises a question as to the validity of certificates issued by foreign certification authorities, which could be a substantial legal issue in cross-border transactions.

Electronic Signatures/Digital Identity Schemes

E-signatures are regulated under the EIT Law and GR 71. They are considered a form of electronic certification and must be issued by a certification authority. The certification authority for electronic certification may either be an Indonesian certification authority or a foreign certification authority. However, the classification of e-signatures produced by these two different authorities differs in evidentiary value before the Indonesian court. An Indonesian certification authority is able to produce a "certified e-signature", whereas a foreign certification authority is only able to produce a "non-certified e-signature" which has less evidentiary value in court.

Currently, several certification authorities have been registered with the MCIT, which is indicative of the MCIT's efforts in promoting the use of e-signatures in Indonesia.

9. Gaming Industry

9.1 Regulations

The Indonesian government has turned its attention towards the gaming industry in the past few years. Last year, the government issued a key regulatory framework on gaming – that is, Presidential Regulation No 19 of 2024 on the Acceleration of the Development of the National Gaming Industry. This regulation aims to boost the share of local game developers and enhance Indonesia's position in global gaming markets.

In the same year, the MOCD issued Regulation No 2 of 2024 on Games Classification (MR 2), which serves as the main reference for game publishers in publishing games.

Age Ratings and Content Restrictions

MR 2 provides game classifications based on age group: 3+, 7+, 13+, 15+ and 18+. The classification is determined based on the following content elements: cigarettes and/or electronic cigarettes, alcoholic beverages, narcotics, psychotropic substances and/or other addictive substances; violence; blood; mutilation and cannibalism; strong language; adult humour; display of human-like characters; pornography; gambling simulation; horror; online interaction; and financial transaction.

In addition to game classifications, game operators are also subject to prohibitions under the EIT Law, GR 71 and MR 5 to display or facilitate the distribution of prohibited content.

In-Game Purchases, Loot Boxes and Gambling Elements

The proliferation of online gambling in Indonesia over past few years has been a significant concern of the government. The regulator and law enforcement authorities have taken an aggressive approach towards combatting online gambling, including performing "cybersweeping" to block online gambling websites. While real online gambling is strictly prohibited under the EIT Law, MR 2 allows gambling simulation games, provided that the game does not have cash-out mechanisms (either in the form of money or prizes).

In making their games available in Indonesia, game developers need to carefully design them to ensure that features like in-game purchases and loot boxes do not include any mechanisms for players/users to exchange them with real money or anything with real-world value.

9.2 Regulatory Bodies

The MOCD acts as the primary regulatory body overseeing the gaming industry.

With regard to game classifications, MR 2 grants the MOCD the authority to:

- revoke a game classification if it is found that the self-assessment result is non-compliant; and
- enforce administrative sanctions in the form of written warnings, temporary suspension and access blocking.

The EIT Law and MCIT Regulation No 7 of 2016 on Administration of Investigation and Prosecution of Criminal Acts in the Field of Information Technology and Electronic Transactions also grant authority to civil servant official investigators to investigate criminal acts in the field of IT and electronic transactions, including instructing the ESO to temporarily terminate access to social media accounts, bank accounts, electronic money and/or digital assets.

The authority is currently very active in enforcing gambling prohibitions, especially in relation to online games. Based on a press release issued by the MOCD, they have blocked access to 5.5 million pieces of online gambling content as of December 2024.

9.3 Intellectual Property

Game developers in Indonesia may encounter several IP challenges that can impact their creative processes and business operations. Common key challenges include the following.

- Copyright infringement: The unauthorised use or reproduction of game assets, such as graphics, music and code, is prevalent and undermines developers' IP rights. This issue is often driven by insufficient legal deterrents and a lack of public understanding or awareness of copyright protections.
- Trade mark disputes: Disputes can commonly arise when brands, characters or titles are used without proper registration or due diligence due to the first-to-file system in Indonesia, which may lead to bad-faith trade mark registrations.
- Piracy (unauthorised distribution): The unauthorised distribution of games, both physical and digital, remains prevalent due to the availability of pirated platforms and insufficient monitoring of digital marketplaces.
- Lack of enforcement and/or awareness of IP protection: Copyright registration is not mandated by regulations, which may give rise to weak enforcement mechanisms and limited awareness of IP rights among consumers and businesses, undermining the protection of developers' rights and allowing IP violations to persist.

IP Rights for Creators in Virtual Environments

Under Indonesian law, creators can take several measures to protect their IP if violations occur.

- Civil measures: Creators may issue a subpoena to the party engaging in infringement, requiring them to cease the violation and provide compensation. If such infringement persists, the creators have the option to initiate a civil lawsuit in the Commercial Court or arbitration (if agreed upon by the parties) to seek the restoration of their rights and claim damages.
- Administrative measures: During the registration of an IP, there are several administrative measures that can be taken by creators to protect their creations. For instance, in case of a trade mark, creators may file an appeal or objection to registration or decisions per-

taining to an IP to the Directorate General of Intellectual Property (DGIP).
- Criminal measures: Article 120 of the Copyright Law establishes that copyright infringements are complaint offences, meaning that criminal proceedings can only be initiated after a formal complaint requesting prosecution of a specific individual or party is filed. Legal actions for copyright violations may be brought before the chairperson of the Commercial Court.

Key Copyright and Trade Mark Considerations in Relation to Digital and Virtual Assets

Video games constitute creations that may be protected under copyright law. Therefore, creations in the form of digital and virtual assets are also covered. Although it must be understood that the registration of an IP and/or any form of digital or virtual asset is not mandatory, such asset or IP may only be protected under copyright law.

Key considerations in the definition of ownership in collaborative projects, and in the marketing or distribution process, include ensuring the creation's originality to guarantee the legal standing of both the moral and economic rights granted by copyright law.

In consideration of the foregoing, while registering an IP with the DGIP is not mandatory, it is strongly recommended that video game content creators register their IP to obtain certain legal protections under Indonesian law.

Trade mark law also provides protection for trade marks created by video game developers, including logos, brands and other identifiers associated with video games produced to aid the trade of goods and/or services.

IP Rights for User-Generated Content

The applicability of IP rights to user-generated content (UGC) may depend on the particular scenario. UGC refers to content created by individuals or consumers, including images, videos, audio and/or text, which is generally created and shared by users instead of a platform operator.

Pursuant to copyright law, the copyright of a creation is retained by the creator unless otherwise specified in the applicable terms or contract. IP rights to UGC generally remain with the creator, although the creator may grant certain licensing rights to third parties for the utilisation of such content. Another scenario is where a creator is specifically instructed by a platform operator to create content, which the parties may determine is "made to order"; thus, the IP rights are retained by the platform operator.

The extent to which platform operators can use UGC depends on the terms and conditions agreed upon by the platform and the creator. Thus, it is important for the platform to clearly specify and establish the scope of IP rights licensing related to UGC in their terms of service.

10. Social Media

10.1 Laws and Regulations for Social Media

The regulation of social media in Indonesia is governed by several legal frameworks that set out the basis for usage, responsibilities and content moderation in social media. Key laws such as the EIT Law, PDP Law and related government regulations reflect the country's commitment to fostering a secure and ethical digital environment. The principal regulations relevant to social media in Indonesia are as follows:

- the EIT Law, which regulates the utilisation of electronic information and transactions in the context of social media, including sanctions for criminal acts perpetrated via the internet (defamation, hate speech, etc);
- GR 71, which establishes operational guidelines applicable to ESOs such as social media platforms – this regulation strengthens government oversight over digital social media by mandating specific obligations and includes prohibition of the distribution of unlawful electronic information or documents;
- MR 5, which imposes requirements regarding the takedown of unlawful content distributed via the internet, including through social media – MR 5 requires platforms to monitor their content actively, and to promptly remove prohibited content flagged by the MOCD, and the regulation provides tight time frames for platforms to comply with TDRs (ie, 24 hours, or four hours for urgent unlawful content; otherwise, platforms will be subject to administrative fines and access blocking); and
- the PDP Law, which focuses on user privacy and data security and is thus critical for social media platforms that handle vast amounts of personal information.

While these regulations provide a framework for the use of social media, key challenges such as content moderation and child protection have emerged as critical areas requiring greater attention.

10.2 Regulatory and Compliance Issues

The main regulatory body with the authority to oversee the use and operation of social media in Indonesia is the MOCD. Under the EIT Law and MR 5, the MOCD has the legal authority to determine unlawful content and issue TDRs to social media platforms for unlawful content. The request can be issued based on a report from the public, other ministries or institutions, law enforcement authorities or judicial institutions.

Similar to the gaming industry, civil servant official investigators also have the authority to investigate criminal acts in the field of IT and electronic transactions, including in relation to social media.

An example of social media enforcement in Indonesia is provided by the actions taken by the MOCD, which actively blocks websites and social media platforms that contain prohibited content in accordance with prevailing laws and regulations. In a notable recent case, the MOCD blocked several social media influencers' accounts that promoted online gambling in 2024. This enforcement highlights the government's efforts towards tackling harmful content on social media, particularly by curbing online gambling through actions against individuals promoting illegal activities.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Rob.Thomson@chambers.com