Legal 500
Country Comparative Guides 2024

Japan
TMT

Contributor

Nagashima Ohno & Tsunematsu

Keiji Tonomura

Partner | keiji_tonomura@noandt.com

Minh Thi Cao Koike

Counsel | minhthi_caokoike@noandt.com

Hiroya Nadamoto

Associate | hiroya_nadamoto@noandt.com

Anju Yamamoto

Associate | anju_yamamoto@noandt.com

This country-specific Q&A provides an overview of tmt laws and regulations applicable in Japan.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

Japan: TMT

1. Is there a single regulatory regime that governs software?

No, there is no single regulatory regime that governs software in Japan.

2. How are proprietary rights in software and associated materials protected?

Under Japanese law, computer software may be legally protected by patents or copyrights.

Under the Patent Act, a computer program, including any information that is to be processed by a computer and is equivalent to a computer program, can be protected where the software program fulfils the requirements of an invention, which is defined as a highly advanced creation of technical ideas utilizing the laws of nature. Registration is required to secure patents or exercise patents with respect to third parties.

While patents protect the ideas underlying computer software, copyrights protect the expression of those ideas. Copyrights provide the copyright owners of certain works (including computer programming works) with certain exclusive rights, including the right to reproduce, distribute, transfer and create derivative works of the software. Registration is not required to secure copyrights or exercise copyrights with respect to third parties, but registration is required to assert the transfer of copyrights against third parties, although conducting such registration is uncommon in practice.

3. In the event that software is developed by a software developer, consultant or other party for a customer, who will own the resulting proprietary rights in the newly created software in the absence of any agreed contractual position?

Unless otherwise stipulated in a contract with a software developer or consultant, the patents and the copyrights will vest in the inventor or the creator, respectively.

Notwithstanding the foregoing, under Article 15 of the Copyright Act, if a work of computer programming is created by a person engaging in the business of a corporation at the initiative of the corporation in the course of the performance of his/her duties, the copyright of such work will vest in the corporation unless otherwise stipulated in a contract or elsewhere at the time the work is made. Although the “person engaging in the business of a corporation” is not limited to a person who has entered into an employment agreement with the corporation, external independent contractors and third parties usually do not qualify as such person engaging in the business of a corporation, unless his/her engagement can be deemed substantially the same as employment relationship.

4. Are there any specific laws that govern the harm / liability caused by Software / computer systems?

There are no specific laws applicable to the liability caused by software or computer systems. While the general law for product liability, the Product Liability Act, does not govern intangibles such as software, it may apply to software or computer systems if they are incorporated in hardware products.

5. To the extent not covered by (4) above, are there any specific laws that govern the use (or misuse) of software / computer systems?

The Act on Prohibition of Unauthorized Computer Access prohibits unauthorized access including inputting someone else's identification information and evading access control features, and the Penal Code stipulates “Crimes Related to Electronic or Magnetic Records Containing Unauthorized Commands", which includes the act of creation and distribution of computer viruses.

6. Other than as identified elsewhere in this overview, are there any technology-specific laws that govern the provision of software between a software vendor and customer, including any laws that govern the use of cloud technology?

In Japan, there are no specific laws that directly prohibit, restrict or otherwise govern software transactions or cloud technology. If the data being placed in the cloud is personal data, use of cloud-based services may be

considered as constituting the provision of personal data to third-parties under the Act on the Protection of Personal Information ("APPI"), which requires the prior consent of the relevant individual (subject to certain exceptions depending on whether such third-parties are located in or outside of Japan). However, the guidelines published by the Personal Information Protection Commission ("PPC") provide that the use of cloud services to store personal data does not constitute the provision of personal data to cloud service providers under the APPI as long as it is ensured by contract or otherwise that the cloud service providers will not handle the personal data stored in the cloud and the cloud service providers are properly restricted from accessing such personal data.

Aside from the personal data protection regulations, provision or use of cloud-based services may be subject to other restrictions depending on the nature of the services or the stored data, including consumer protection regulations and sector-specific guidelines in medical and financial sectors, such as Version 1.1 of the Safety Management Guidelines for Providers of Information Systems/Services for Medical Information, published by the Ministry of Economy, Trade and Industry ("METI") in July, 2023. The Information Security Management Guidelines for the Use of Cloud Services (2013), published by the METI in March 2014, provides advice for the selection and implementation of appropriate controls from the ISO Q 27002 (code of practice) and guidance for optimal implementation in order to address risks associated with the use of cloud services. Also, the Information Security Measures Guidelines for the Provision of Cloud Services (3rd edition, 2021) published by the Ministry of Internal Affairs and Communications ("MIC") in September 2021, provides advice for cloud service businesses to address risks associated with the provision of IoT or cloud services, the Guidelines for Appropriate Settings for the Use and Provision of Cloud Services published by the MIC in October 2022, provides advice for security measures for both users and providers, and the Guidebook for Preventing Mistakes When Setting Up Cloud Services published by the MIC in April 2024, provides advice to users of cloud services on measures to prevent mistakes in connection with the set-up of cloud services.

7. Is it typical for a software vendor to cap its maximum financial liability to a customer in a software transaction? If 'yes', what would be considered a market standard level of cap?

It is common for SaaS agreements to have a clause to limit maximum financial liability of a vendor to a customer, while such clause is not typical in a software license agreement. The cap amount is usually set forth as the amount equivalent to the service fee for 6 months or 12 months.

8. Please comment on whether any of the following areas of liability would typically be excluded from any financial cap on the software vendor's liability to the customer or subject to a separate enhanced cap in a negotiated software transaction (i.e. unlimited liability): (a) confidentiality breaches; (b) data protection breaches; (c) data security breaches (including loss of data); (d) IPR infringement claims; (e) breaches of applicable law; (f) regulatory fines; (g) wilful or deliberate breaches.

Among the areas of liability above, wilful or deliberate breaches are typically excluded. Also, according to Article 8(1) of the Consumer Contract Act, clauses that exempt the vendor from all liability or exempt the vendor from part of its liability that arises due to its wilful act or gross negligence are invalid. Other areas of liability may be excluded from the liability cap in cross border contracts, but are typically not excluded in domestic transactions.

9. Is it normal practice for software source codes to be held in escrow for the benefit of the software licensee? If so, who are the typical escrow providers used? Is an equivalent service offered for cloud-based software?

The Software Information Center (SOFTIC) is a major escrow agent for software source codes. As of March 31, 2022, SOFTIC's services had been used only for 395 contracts; given the small number of users, it cannot be said that use of these escrow services is normal practice. SOFTIC also offers services for cloud-based software by receiving deposit of source codes and other materials.

10. Are there any export controls that apply to software transactions?

The Foreign Exchange and Foreign Trade Act provides for a permit system by the METI for transactions in which certain technologies, including programs, specified in the Foreign Exchange Order ("specified technology") are provided to or in a foreign country. For example, the provision of certain cryptographic technologies in a

foreign country is subject to those regulations.

Uploading data containing specified technology to a cloud server located in a foreign country does not constitute a transaction requiring a permit as long as the purpose is for the cloud service user to use the data for its own purposes. On the other hand, if, in substance, the purpose is to provide specified technology to a cloud service provider or a third party, the act of uploading the data is subject to the regulations.

SaaS that provides specified technology constitutes a transaction that requires a permit. However, for services that provide a program that is commercially available, a permit is not required if the requirements of the Ministerial Ordinance on Trade Related Invisible Trade, etc. are met (e.g., in the case where it is designed so that technical assistance of the distributor is not required).

11. Other than as identified elsewhere in this questionnaire, are there any specific technology laws that govern IT outsourcing transactions?

There are no specific laws that govern IT outsourcing transactions, but general laws could be applicable to outsourcing transactions. For example, under the Act against Delay in Payment of Subcontract Proceeds, etc. to Subcontractors, which aims to protect the interests of subcontractors in a weak bargaining position, large procuring enterprises are obligated to deliver documents to subcontractors that contain matters required by the Act. In addition, if the outsourced individual is treated as the company's own employee, it may violate the Act on Securing the Proper Operation of Worker Dispatching Businesses and Protecting Dispatched Workers. Furthermore, the Act on Optimization, etc. of Transactions concerning Specified Consignees, commonly referred to as the "Freelance Protection Act," which was promulgated on May 12, 2024, requires certain business operators that outsource their business to freelancers, among other obligations, to clearly state the conditions of the transaction, to pay the compensation within 60 days, and to establish a system to prevent harassment.

12. Please summarise the principal laws (present or impending), if any, that protect individual staff in the event that the service they perform is transferred to a third party IT outsource provider, including a brief explanation of the general purpose of those laws.

Under the Act on the Succession to Labor Contracts upon Company Split, in the case where the parties agree to transfer a certain business (including employees, assets, third-party contracts and/or liabilities) by way of a company split (kaisha-bunkatsu), employees who are primarily engaged in the transferred business but who will not be transferred, and employees who are not primarily engaged in the transferred business but who will be transferred, are entitled to certain opt-out rights concerning their non-transfer or transfer, respectively. The purpose of this law is to protect employees who will be significantly affected by the succession of their labor contract.

Also, in the case where the parties agree to transfer a certain business by way of a business transfer or merger, the parties are recommended to comply with the guidelines concerning the matters that should be noted by companies upon business transfer or merger, which was established by the Ministry of Health, Labour and Welfare.

13. Please summarise the principal laws (present or impending), if any, that govern telecommunications networks and/or services, including a brief explanation of the general purpose of those laws.

The principal law governing telecommunications networks and services in Japan is the Telecommunications Business Act (the "Act"). The primary purpose of this Act is to ensure the efficient provision of telecommunications services, promote fair competition among service providers, and protect the interests of users. It is notable that the Act also may apply to a foreign entity that provides telecommunications services for customers in Japan from abroad, in which case the foreign entity is required to appoint a representative or agent in Japan.

A summary of the Act is as follows:

- General rules: Telecommunications carriers are prohibited from censorship of information and are required to protect the secrecy of communications.
- Rules related to entry: Those who wish to engage in the telecommunications business must register with or notify MIC in advance according to the content of their telecommunications business. The definition of the telecommunications business that requires registration or notification is complex, but in general, those who (i) install telecommunications line facilities or (ii) mediate others' communications are required to

register or notification. Telecommunications businesses that do not fall under either (i) or (ii) (the scope of these telecommunications businesses is broad, including many social networking services, online shopping malls, online search engines, and various online information provision services) do not require registration or notification. However, they must comply with certain regulations under the Act, such as rules related to user information described below.

- Rules related to consumer protection: The Act provides rules for consumer protection that telecommunications carriers and agents must comply with, such as explaining the terms of service to users, providing written documents to users, and informing users when intending to suspend or discontinue telecommunications services.
- Rules related to user information: Telecommunications carriers are subject to rules regarding the external transmission of user information. Also, telecommunications carriers providing telecommunications services to a large number of users would be subject to certain rules for the proper handling of specific user information, such as the establishment of information handling policies, and the self-evaluation of handling of specific user information.
- Rules related to telecommunications facilities: Telecommunications carriers who install telecommunications line facilities, and those who provide large-scale paid telecommunications services, are subject to rules concerning telecommunications facilities used for the telecommunications business, such as maintaining compliance with technical standards.
- Rules related to reporting: Telecommunications carriers are required to promptly report when there are certain leaks of specific user information as defined in the Act.

14. What are the principal standard development organisations governing the development of technical standards in relation to mobile communications and newer connected technologies such as digital health or connected and autonomous vehicles?

In the global field of information and communications, there are de jure standards created by international standardization organizations such as the International Telecommunication Union (ITU), the International Organization for Standardization (ISO), and the International Electrotechnical Commission (IEC), as well as de facto standards created by private organizations such as the Internet Engineering Task Force (IETF), the Institute of Electrical and Electronics Engineers, Inc. (IEEE), and the World Wide Web Consortium (W3C). In Japan, in addition to the above organizations, there are private standardization organizations that create voluntary standards, including the Telecommunication Technology Committee (TTC), the Association of Radio Industries and Businesses (ARIB), and the Japan Cable Television Engineering Association (JCTEA).

15. How do technical standards facilitating interoperability between connected devices impact the development of connected technologies?

Standardization of information and communication services, including connected devices, refers to a series of efforts aimed at achieving common specifications for both hardware and software across networks, including terminal equipment, switches, and multiplexing devices. The effects of standardization include not only ensuring interoperability and interconnectivity but also enabling mass production of equipment and systems, leading to lower prices and increased user benefits. Additionally, it facilitates the efficient provision of information and communication services and promotes competition through the entry of new business operators and manufacturers into the market.

16. When negotiating agreements which involve mobile communications or other connected technologies, are there any different considerations in respect of liabilities/warranties relating to standard essential patents (SEPs)?

Before the 5G era, negotiations for SEPs were primarily conducted between telecommunications companies. At the time, most licensees were companies engaged in the research and development of telecommunications technology, enabling license negotiations among parties with a deep understanding of the technology. With the advent of 5G and the development of new services using IoT, companies from various industries that do not engage in telecommunications technology R&D and do not hold SEPs have started to use the 5G standard. Licensing negotiations for SEPs in the field of information and communication technology across different industries present various concerns, such as difficulty in resolving issues through cross-licensing, challenges in evaluating the scope, essentiality, and value of each other's patents, and differing perspectives on appropriate

royalty rates, which complicate negotiations.

In response to these concerns, the Japan Patent Office developed the "Guide to Licensing Negotiations Involving Standard Essential Patents" in June 2018 (revised in June 2022) to enhance the transparency and predictability of licensing negotiations for SEPs necessary for implementing standards in fields such as wireless communications, to facilitate negotiations between patent holders and implementers, and to prevent and resolve disputes at an early stage. Additionally, in March 2022, the Ministry of Economy, Trade, and Industry (METI) established the "Good Faith Negotiation Guidelines for Standard Essential Patent Licensing" to present norms for good faith negotiations for SEP licensing involving domestic patents, aiming to ensure a fair transaction environment by improving transparency and predictability of licensing negotiations.

While these guidelines are not legally binding and do not constrain court decisions, they outline the issues in SEP licensing negotiations both domestically and internationally, as well as Japan's norms for good faith negotiations. Although, the guidelines do not provide specific details on liabilities/warranties, they highlight the following issues concerning liabilities/warranties: When a SEP holder demands royalties after the sale of the final product, it may become an issue how the payment of royalty should be allocated within the supply chain. Final product manufacturers may have pre-existing patent indemnity agreements with suppliers stipulating that the supplier bears the obligation to pay royalties. In such cases, even if the royalties negotiated by the final product manufacturer with the SEP holder are excessive compared to the supplier's component price, the supplier may nevertheless be required to pay the royalty based on the indemnity agreement. To avoid such situations, suppliers may have to negotiate to exclude SEPs from patent indemnity agreements. Additionally, the guidelines discuss the view that the allocation of royalties within the supply chain should be decided based on who has the core inventive elements of the patent within a supply chain to avoid placing an excessive burden on suppliers.

17. Which body(ies), if any, is/are responsible for data protection regulation?

The Personal Information Protection Commission ("PPC") is responsible for data protection regulations.

18. Please summarise the principal laws (present or impending), if any, that that govern data protection, including a brief explanation of the general purpose of those laws.

The Act on the Protection of Personal Information ("APPI") contains a comprehensive, cross-sectional framework for the protection of personal information, which regulates the use of personal information by both the public and private sectors. The APPI is implemented by cross-sectional administrative guidelines prepared by the PPC. With respect to certain sectors, such as medical, financial and telecommunications businesses, sector-specific guidance and guidelines are published by the relevant governmental ministries jointly with the PPC given the highly sensitive nature of personal information handled in those sectors.

19. What is the maximum sanction that can be imposed by a regulator in the event of a breach of any applicable data protection laws?

Under the APPI, there is no administrative fine for the breach of the APPI; however, criminal penalties may be imposed on business operators handling personal information under certain circumstances. The maximum criminal fine that can be imposed on corporations is JPY 100,000,000, in situations where business operators violate either (i) the prohibition against theft or illegal provision of a personal information database or (ii) a PPC order.

20. Do technology contracts in your country typically refer to external data protection regimes, e.g. EU GDPR or CCPA, even where the contract has no clear international element?

Technology contracts without international elements does not usually refer to external data protection regimes, while they may be referred in cross-border transactions.

21. Which body(ies), if any, is/are responsible for the regulation of artificial intelligence?

There is no regulatory body that plays a leading role in regulating AI.

Instead, several ministries and agencies are primarily responsible for the enforcement of AI-related laws under their jurisdiction based on the relevant sector. As part of a soft law approach, the MIC and the METI published the "AI Guidelines for Business Operators" on April 19, 2024 (see question 22). In addition, several government bodies, such as the Cabinet Office and the Digital Agency, have

been discussing issues related to the promotion of AI development and concerns about its use.

In the public sector, the Japan AI Safety Institute ("AISI") has been established in the Information-technology Promotion Agency (IPA). AISI is responsible for (i) investigating and discussing standards for safety assessment, (ii) discussing methods of conducting safety assessment, and (iii) engaging in international cooperation with relevant institutes in other countries such as the AI Safety Institute in the US and the UK.

22. Please summarise the principal laws (present or impending), if any, that that govern the deployment and use of artificial intelligence, including a brief explanation of the general purpose of those laws.

Although the implementation of a new regulatory regime for artificial intelligence has been discussed (see questions 29), there are currently no comprehensive laws governing artificial intelligence. However, in some sectors, relevant laws regulate the deployment and use of artificial intelligence. For example, in the medical device sector, there is a move to accommodate AI-enabled medical devices under the Pharmaceutical and Medical Devices Act. In relation to automated driving, the Road Traffic Act establishes relevant rules, including a permit system for Level 4 automated driving.

In addition, the "AI Guidelines for Business Operators" were published on April 19, 2024. While these guidelines are not legally binding, they represent soft-law with a goal-based approach, based on other existing three guidelines on AI ("Governance Guidelines for Implementation of AI Principles", "AI R&D guidelines for international discussions", and "AI Utilization Guidelines"). Business operators engaged with AI are expected to voluntarily promote specific initiatives, such as establishing appropriate AI governance. An overview of the guidelines is as follows:

- The entities covered by the guidelines are broadly classified into three categories: (i) "AI Developers" (including entities that study AI), (ii) "AI Suppliers" (entities that provide services incorporating AI), and (iii) "AI Users" (entities that use AI systems or AI services).
- The guidelines present ten principles that are common to the entities subject to the guidelines, and points of emphasis in AI activities are specified based on the category of such The ten principles are: (i) human-centric, (ii) safety, (iii) fairness, (iv) protection of privacy, (v) security, (vi) transparency, (vii) accountability, (viii) education and literacy, (ix) fair competition, and (x) innovation.
- The appendix to the guidelines includes the following:
    - examples of AI services (including relationships among entities);
    - AI benefits and possibilities, specific examples of risks;
    - practical points for developing AI governance and practical examples;
    - commentaries based on the three categories (AI developers, AI suppliers, and AI users), examples of specific methods for implementing the guidelines, and easy-to-understand references; and
    - checklist for business operators for compliance with the guidelines.

23. Are there any specific legal provisions (present or impending) in respect of the deployment and use of Large Language Models and/or generative AI?

There is no general legal regime governing the deployment and use of Large Language Models and/or generative AI; however, there are certain provisions of relevant laws and regulations. For instance, with respect to the use of copyrighted works in the development of AI, in certain cases where the use is not intended to enjoy the thoughts or sentiments expressed in the copyrighted work, copyright protection will not apply and such use is not considered copyright infringement, with certain exceptions, under Article 30- 4 (ii) of the Copyright Act. Under this rule, use of third-party copyrighted works for the purpose of "AI learning" for generating AI-created work does not usually constitute copyright infringement. As for the issues under the Copyright Act including the above provisions in the context of generative AI, the Agency for Cultural Affairs published a paper entitled, "General Understanding on AI and Copyright in Japan" on March 15, 2024. This paper is not legally binding.

24. Do technology contracts in your jurisdiction typically contain either mandatory (e.g mandated by statute) or recommended provisions dealing with AI risk? If so, what issues or risks need to be addressed or considered in such provisions?

As there are currently no comprehensive laws governing artificial intelligence, we have not identified any typical mandatory provisions dealing with AI.

As for recommended provisions, there are no provisions typically contained in technology contracts; however, there are several provisions used to mitigate risks related to AI.

In the training and development phase of AI, if the data used for the process infringe on the rights of third parties, the training or development, or outputs of such AI may infringe on such rights of third parties. Therefore, in some cases, a provider of data provides representations and warranties stating that use of the data does not infringe on the rights of third parties including intellectual property rights. In contracts that are favourable to providers of data, on the other hand, such warranties can be disclaimed in addition to the disclaimer of accuracy and completeness of data.

In the generation and use phase, there is a risk that the outputs of AI may not be copyrighted works. Thus, in some outsourcing contracts, the consignee is prohibited from using AI in order to allow the consignor to obtain copyright for the deliverables

The AI section of the "Contract Guidelines on Utilisation of AI and Data Version 1.1" (2019) published by the METI explains factors to consider and methods to prevent issues including some of the above, for contracts that concern the development and utilisation of AI-based software. The Contract Guidelines are supplemented by the appendix to the "AI Guidelines for Business Operators" in consideration of changes to the development and utilisation of AI since the publication of the Contract Guidelines.

25. Do software or technology contracts in your jurisdiction typically contain provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs in the context of the use of AI systems?

Provisions regarding the application or treatment of copyright or other intellectual property rights, or the ownership of outputs can be found in contracts and terms and conditions for AI that is broadly provided to general users. In many cases, the rights and ownership are vested in users subject to certain conditions of usage.

26. What are the principal laws (present or impending), if any, that govern (i) blockchain specifically (if any) and (ii) digital assets, including a brief explanation of the general purpose of those laws?

There are no laws that govern blockchain specifically.

Regarding digital assets, if the assets constitute security tokens, then the regulations related to securities will apply under the Financial Instruments and Exchange Act ("FIEA").

Shares and bonds represented in tokens and electronically recorded transferable rights are classified as securities which are required to be handled by Type I Financial Instruments Business Operators and are subject to disclosure rules. Security tokens that are subject to technological restrictions on transfer may fall into another type of securities.

As for the digital assets which fall under crypto-assets, the crypto-asset exchange services are regulated under the Payment Services Act (-"PSA"). Stablecoins are also subject to the regulations under the PSA. Certain stablecoins are classified as electronic payment instruments and the PSA regulates the intermediaries of stablecoins.

Further, from the perspective of anti-money laundering, certain services handling digital assets are subject to the Act on Punishment of Organized Crime and Control of Proceeds of Crime.

27. Please summarise the principal laws (present or impending), if any, that govern search engines and marketplaces, including a brief explanation of the general purpose of those laws.

The Telecommunications Business Act governs both search engines and marketplaces. Separately, multiple laws related to online sales, advertising, and platforms apply with respect to marketplaces.

- Regulations under the Telecommunications Business Act

Under the Telecommunications Business Act, large-scale internet search engines and large-scale social media service providers with at least 10 million monthly users that are designated by the Minister of MIC must make a telecommunications business filing and comply with certain regulations under the Act. Marketplaces are not subject to these requirements.

Further, the Minister of MIC may designate telecommunications carriers (including search engines and marketplaces) as providing telecommunications

services that have a significant large number of users (at least 10 million users for free services and at least 5 million users for paid services). If so designated, such telecommunication carriers must properly handle specific user information (i.e., (i) information protected under secrecy of communications and (ii) certain searchable information that can identify users).

Further, when certain telecommunications carriers stipulated in Regulations for Enforcement of the Telecommunications Business Act (including search engines, marketplaces, and social media services) send certain programs to users' devices to transfer such users' information stored in their devices (such as third-party cookies, tags, and advertising IDs) externally, they must give prior notification to the users of the content of the user information that is to be sent externally, the destination of such information, and the purpose of use of such information, or place the user in a position where they can obtain such information.

- Regulations Related to Marketplaces

Under the Act on Specified Commercial Transactions, regarding online sales, it is obligatory for businesses to display important information when advertising, and false or exaggerated advertisements are prohibited. Furthermore, the Act against Unjustifiable Premiums and Misleading Representations prohibiting businesses from making inappropriate advertisements or representations that could mislead consumers and offering excessive benefits that could distort consumer judgement.

Under the Act on the Protection of Consumers Who Use Digital Platforms for Shopping, obligations are imposed on "digital trade platforms (DTPs)" such as online malls, to make efforts to implement certain measures to address issues related to online sales transactions conducted using the DTP and resolve disputes. Furthermore, DTPs are obliged to publicly disclose an outline and implementation status of such measures.

Under the Act on Improving Transparency and Fairness of Specified Digital Platforms, the Minister of Economy, Trade and Industry designates businesses that provide platforms exceeding a certain size as "specified digital platform providers". The designated "specified digital platform providers" are obliged to (i) disclose information such as commercial terms, (ii) ensure fairness in business operations, and (iii) report on the status of their business operations. As for the platform providing online mall or app stores, three online mall operators (Amazon, Rakuten, Yahoo) and two app stores (Apple, Google) have been designated as specified digital platform providers to date.

28. Please summarise the principal laws (present or impending), if any, that govern social media, including a brief explanation of the general purpose of those laws?

While there are no laws that specifically govern social media, the Telecommunications Business Act and the Provider Liability Limitation Act are closely related to social media.

Providers of social media services generally fall under the category of telecommunications carriers and have a duty to protect the secrecy of users' communications. Services that mediate the communications of others using telecommunications equipment are generally required to file a notification under the Telecommunications Business Act. The provision of a direct chat function would correspond to the mediation of others' communication. Therefore, social media services with a direct chat feature must file a notification under the Telecommunications Business Act (even without a direct chat feature, as stated in #26, large-scale social media services need to make a notification). As described in #26, obligations related to specified user information in the case of telecommunications services with a significant large number of users and obligations related to the external transmission of information regarding users also apply to social media services.

The Provider Liability Limitation Act sets out the requirements for exemption from civil liability for telecommunications providers (including social media) in the event that information infringing on the rights of third parties ("rights-infringing information") is posted on social media. The Provider Liability Limitation Act sets out certain conditions for the provider to be exempted from civil liability in the case where (i) the provider deletes the rights-infringing information without the consent of those who post it or (ii) the provider does not delete the rights-infringing information. Furthermore, the Act allows the relevant third-party to request the provider to disclose information regarding the party that posted the rights-infringing information.

In addition, the National Diet in 2024 passed a bill amending the Provider Liability Limitation Act. Under this amendment, the Provider Liability Limitation Act will become a part of the Information Distribution Platform Act which is scheduled to take effect by May 17, 2025. Under the Information Distribution Platform Act, certain large-scale web media, such as social networking services (SNS) designated by the Minister of Internal Affairs and Communications, are required to fulfill the following obligations:

1. Publicize the method for receiving requests from infringed persons (those whose rights have been violated by information distributed on the web media).
2. Investigate the infringing information: When an infringed person requests the large scale web media to take measures to prevent the transmission of infringing information, the large scale web media shall promptly conduct an investigation.
3. Appoint and register specialists to investigate infringing information.
4. Notify the requester: Within 14 days from the date of receipt of the request from an infringed person, notify the requester of the results of the investigation and whether measures will be taken to prevent the transmission of infringing information.
5. Publicize the standards for implementing measures to prevent transmission.
6. Notify those who post the information when action is taken to prevent the transmission of infringing information.

29. What are your top 3 predictions for significant developments in technology law in the next 3 years?

In the near future, we expect developments in the fields of (i) ride-hailing, (ii) AI, and (iii) web 3.

As for ride-hailing, on March 29, 2024, the Ministry of Land, Infrastructure, Transport and Tourism ("MLIT") established a new regime allowing for the provision of paid transportation services by local private vehicles and non-professional drivers under the management of taxi business operators ("Private Vehicle Utilization Business"), and issued guidelines regarding permits for the provision of such services under the Road Transport Act. The Private Vehicle Utilization Business regime has been seen as partially lifting ride-hailing restrictions in Japan.

As for ride-hailing business operated by non-taxi companies, the "Report on the Promotion of Regulatory Reform – User-Driven Social Change -" published by the Council for Regulatory Reform in the Cabinet Office on May 31, 2024 proposed that the government start drafting a bill allowing for ride-hailing businesses operated by non-taxi companies. This was followed by the "Basic Policy for Economic Management and Reform 2024" decided by the Cabinet on June 21, 2024 stating that the government will discuss methods to allow such ride-hailing business including the legislative regime.

As for AI, the "Project Team on the Evolution and Implementation of AIs" in the Liberal Democratic Party, published "the AI White Paper 2024 New Strategies in stage II – To the most AI-Friendly Country in the World -" in April 2024. The White Paper proposes strategies to strengthen competitiveness of Japan through the use of AI and to ensure safety of AI including a proposal of a legislative regime to regulate significantly high-risk AI, for the purpose of realizing Japan as the "world's most AI-friendly country" with the best understanding of AI and the easiest AI R&D and implementation.

The "Approach to AI Systems" published by the AI Strategy Council in the Cabinet Office in May 2024 suggests a regime based on risks for each category of entities. The basic principle is to regulate entities by soft laws such as the AI Guidelines for Business Operators and a certification system for products and the internal governance system of an entity. In addition, sector specific hard laws are expected to regulate relevant providers and users of AI with great influence and high risk. As for developers of AI with great influence and high risk, this paper recommends a discussion regarding the necessity of a legislative regime to supplement soft laws. The AI System Research Group established in the AI Strategy Council will also discuss the regime for AI in Summer 2024.

As for web 3, the web 3 project team also in the Liberal Democratic Party published the "web3 White Paper – A New Era Where Technology Forms the Foundation of Society– " in April 2024. The White Paper proposed issues that are hindering the execution of web 3-related projects and issues that need to be discussed in order for the web 3 ecosystem to develop and become widespread. For example, it requests the establishment of a new licensing system for intermediaries between users and crypto-assets exchange services or electronic payment instruments services where licensing requirements for the intermediaries are less strict than those for the providers of such services.

30. Do technology contracts in your country commonly include provisions to address sustainability / net-zero obligations or similar environmental commitments?

No, technology contracts do not commonly include such provisions, while ESG is a hot issue in the technology field.

Contributors

Keiji Tonomura
Partner
keiji_tonomura@noandt.com

Minh Thi Cao Koike
Counsel
minhthi_caokoike@noandt.com

Hiroya Nadamoto
Associate
hiroya_nadamoto@noandt.com

Anju Yamamoto
Associate
anju_yamamoto@noandt.com