MORI HAMADA

Tech, IP and Telecoms Law Newsletter

March 28, 2025

This month's contents:

Atsushi Okada
Partner
atsushi.okada@morihamada.com

Daisuke Tsuta
Partner
daisuke.tsuta@morihamada.com

Colin Trehearne
Counsel
colin.trehearne@morihamada.com

Kaei Ro
Counsel
kaei.ro@morihamada.com

Kohei Wachi
Senior Associate
kohei.wachi@morihamada.com

Masumi Sato
Associate
masumi.sato@morihamada.com

Hiromu Nagira
Associate
hiromu.nagira@morihamada.com

We are pleased to present the March 2025 issue (Vol.14) of our Tech, IP and Telecoms Law Newsletter, a collection of the latest information about Japanese technology, intellectual property, and telecommunications law. We hope that you will find it useful to your business.

1. Cabinet Secretariat Submits Bill on Active Cyber Defense

On February 7th 2025, the Cyber Security System Development Preparatory Office of the Cabinet Secretariat submitted a bill on active cyber defense (the Japanese version of Active Cyber Defense: ACD). A bill on the prevention of damage caused by unauthorized acts against important computers (the "**Cyber Response Enhancement Bill**"; hereinafter referred to as the "**New Bill**") and a bill to revise related laws in line with the enforcement of the New Bill (hereinafter referred to as the "**Revision Bill**") (only available in Japanese) were submitted to an ordinary session of the Diet. The content of the New Bill and the Revision Bill is wide-ranging, and is broadly divided into four categories: (1) public-private partnerships (including incident reporting obligations for essential infrastructure providers), (2) use of communication information, (3) access and neutralization, and (4) cross-cutting issues (for more detailed content, please also refer to our Data Security Newsletter (February 2025) (only available in Japanese).

For example, with regard to (1) public-private partnerships, measures will be taken to make incident reporting mandatory for essential infrastructure providers. Essential infrastructure providers are businesses that are individually designated and are from 15 essential infrastructure fields based on the Act on the Promotion of Security by Integrally Taking Economic Measures (the Act on the Promotion of Economic Security). When an essential infrastructure operator introduces a "specified important computer" (a computer used by a essential infrastructure operator that is specified by Cabinet Order as one whose cyber security, if compromised, could cause the control system of the infrastructure or other functions to stop or deteriorate), they must notify the minister in charge of the business of the product name, manufacturer name and other matters specified by the ordinance of the competent ministry.

In addition, when an essential infrastructure provider becomes aware of a "specific infringement event" (such as cyber security being compromised in a specified important computer due to unauthorized access, etc.) or an event specified by the ordinance of the competent ministry that could cause such an event, they are obliged to report this to the minister in charge of the business and to the prime minister, as well as certain other matters specified by ministry ordinance.

2. Ministry of Economy, Trade and Industry Releases its "Evaluation on Transparency and Fairness of Specified Digital Platforms"

On February 14, 2025, the Ministry of Economy, Trade and Industry ("**METI**") compiled an evaluation of the transparency and fairness of designated digital platform providers in three areas: (1) general online shopping malls, (2) app stores, and (3) digital advertising. This evaluation was conducted in accordance with the Act on Improving Transparency and Fairness of Specified Digital Platforms (available here) and was based on reports submitted by providers, information received through consultations, and opinions expressed in monitoring meetings. With respect to the evaluation of the handling of personal data acquired and used for targeted advertising in the digital advertising sector, METI consulted with the Ministry of Internal Affairs and Communications ("**MIC**"), referencing the "Monitoring Results on the Handling of User Information" by MIC's Working Group on User Information.

This marks the third evaluation for (1) general online shopping malls and (2) app stores. While METI acknowledged certain improvements in platform operations based on the efforts of businesses, it also identified remaining challenges in enhancing transparency and fairness. Specifically, individual companies were required to take further corrective actions to address the outstanding issues related to transparency and fairness, including operational improvements and enhanced reporting.

For (3) digital advertising, this is the second evaluation to occur. The report particularly emphasized the need for measures against "spoofed advertisements," where advertisers misrepresent their identity. It was highlighted that ensuring a fair trading environment is essential in addressing this issue. In June 2024, MIC requested large-scale service providers offering social networking services and similar platforms to implement countermeasures against spoofed advertisements. Furthermore, on February 28, 2025, an amendment to the Penal Code was submitted to the ongoing regular session of the National Diet. This proposed amendment aims to criminalize the falsification of electronic data, thereby enabling the prosecution of spoofed advertisements. The bill is currently under deliberation.

3. Bill on the Promotion of Research and Development and the Utilization of AI-Related Technologies

On February 28, 2025, the government submitted the "Bill on the Promotion of Research and Development and the Utilization of AI-Related Technologies" to the National Diet. The purpose of this bill is to promote the research and development of AI, encourage its utilization, and address the associated risks.

This bill outlines the fundamental principles for promoting AI research and development. It recognizes that AI-related technologies are foundational to the advancement of the economic and social landscape and are also crucial from a national security perspective. Therefore, it emphasizes the need to maintain domestic research and development capabilities and enhance international competitiveness. At the same time, the bill highlights the necessity of implementing measures to ensure transparency and address other essential concerns, considering the potential risks AI may pose. The government is required to formulate a basic plan for AI based on these principles and establish a new AI Strategy Headquarters within the Cabinet to oversee the implementation of AI-related policies.

Regarding private enterprises, the bill defines "businesses utilizing AI" as those developing or providing products or services using AI-related technologies or incorporating such technologies into their business activities. The bill requires these businesses to "cooperate" with national and local government initiatives; however, it is currently unclear what this obligation to "cooperate" specifically involves.

The bill does not stipulate penalties such as fines or orders for businesses utilizing AI that do not fulfill the "cooperation" obligation. However, Article 16 states that "*the government shall collect information on domestic and international trends in AI-related technology research, development, and utilization, analyze cases where the rights and interests of citizens have been infringed due to improper or inappropriate AI-related activities, and conduct investigations and research to promote AI-related technology. Based on these findings, the government shall provide guidance, advice, and necessary information to research and development institutions, utilization businesses, and other relevant parties*." This grants the government investigative authority and the ability to provide guidance and advice to businesses utilizing AI.

Additionally, other significant AI policy developments include METI's publication of a "Contract Checklist for

AI Utilization and Development" in February 2025 and the Financial Services Agency's release of a discussion paper in March 2025 on the current state and promotion of sound AI utilization in financial institutions.

Given the centrality of AI to numerous technological and business developments, it is anticipated that discussions on AI-related legal policies will continue to be active. Participants will benefit from paying attention to such discussions, and in particular, debates regarding the enactment of the bill.

4. High Court Judgments Released on Shogi Match Live Video Streaming Records

Recently, two high court judgments released on Shogi match live video streaming records: the Osaka High Court judgment on January 30, 2025 (first instance: Osaka District Court judgment on January 16, 2024, the "**Osaka Case**") and the Intellectual Property High Court judgment on February 19, 2025 (first instance: Tokyo District Court judgment on February 26, 2024, the "**Tokyo Case**").

Both high court judgments involve a YouTuber (plaintiff) who streamed videos (the "**Videos**") that reproduced game record information on Shogi in real-time while watching paid broadcasts of shogi matches by Igo Shogi Channel Co., Ltd. (the "**Igo Shogi Channel**"). The YouTubers' actions led to Igo Shogi Channel filing a request to delete the Videos on the grounds of copyright infringement on their platform (the "**Deletion Request**") and the temporary deletion of the Videos based on this request. The YouTubers then sought an injunction against the Deletion Request under the Unfair Competition Prevention Act and claimed damages based on tort against Igo Shogi Channel.

In the first instance, both courts partially upheld the plaintiff's claims and ordered Igo Shogi Channel to pay damages. However, in the appeals, the Osaka High Court overturned the first instance judgment and dismissed the plaintiff's claims, while the Intellectual Property High Court upheld the first instance judgment and ordered the defendant (Igo Shogi Channel) to pay damages, resulting in two potentially inconsistent judgments.

As of the publication date of this newsletter, the detailed judgment from the Intellectual Property High Court has not yet been released, so the specifics remain to be revealed. However, it is important to note that in the Tokyo Case, the defendant did not contest the alleged infringement under the Unfair Competition

Prevention Act and tort (except for the issue of whether the plaintiff's claimed personal interests are considered "legally protected interests" under Article 709 of the Civil Code), and thus, the infringement argument was not a point of contention.

In the Osaka High Court judgment, the main issue was whether the Deletion Request infringed on the plaintiff's "business interests." The court stated that the plaintiff's streaming of the Videos "hinders the establishment of the business model on which the Japan Shogi Association's revenue structure stands, and ultimately threatens the continuation of shogi matches on the current scale." The court further noted that the plaintiff's streaming of the Videos, which involved obtaining real-time game record information by merely bearing the cost as a viewer and using it to appeal to viewers and generate revenue, (1) intentionally caused damage to the defendant, and (2) clearly fell outside the scope of fair competition. The court recognized the streaming of the Videos as a tort that infringes on the defendant's business interests and dismissed all of the plaintiff's claims, stating that the plaintiff does not have any "business interests" or "business credibility" protected under the Unfair Competition Prevention Act in relation to the streaming of the Videos. This chimes nicely with a recent Tokyo High Court judgment on June 19, 2024 (the Band Score Case), which held that the act of publicly sharing online band scores that were imitations of published and sold band scores constituted a tort of infringing on business interests.

Finally, we note that there is ongoing academic debate about whether game record information on Shogi constitutes a copyrighted work. In the Osaka Case, the defendant (Igo Shogi Channel) did not argue that the game record information on Shogi itself is a copyrighted work, so this issue was neither contested nor judged. However, it is noteworthy that streaming videos that reproduce game record information in real-time can be recognized as a tort outside the scope of fair competition, even if the game record information on Shogi is not considered a copyrighted work. This may be argued to be particularly relevant in relation to the scope of "special circumstances such as infringing legally protected interests that are different from the benefits derived from the use of works regulated by Copyright Act", as stated in the Supreme Court judgment in the North Korean Film Case (Supreme Court First Petty Bench judgment on December 8, 2011, Minshu Vol. 65, No. 9, p. 3275), which examined cases where the use of works not protected by Copyright Act was argued to constitute a tort.

There are various interpretations regarding the "special circumstances" in the Supreme Court judgment in the North Korean Film Case, and it will be necessary to closely monitor future discussions and trends in case law.

5. Supreme Court Rulings in Two Cases Concerning Cross-Border Networked System Find Patent Infringement

On March 3, 2025, the Second Petty Bench of the Supreme Court ruled that two cases of alleged patent infringement involving cross-border networked systems did indeed constitute infringement (Case 1: Supreme Court Second Petty Bench Decision March 3, 2025 (Case No. Reiwa 5 (Ju) 14 and 15), Case 2: Supreme Court, Second Petty Bench, March 3, 2025 (Case No. Reiwa 5 (Ju) 2028)). In both cases, X, the patent holder for a system, program, and device for displaying user comments alongside videos, claimed that Y, a US corporation providing a similar video distribution service via web servers outside Japan, had infringed on their patent rights. X sought an injunction and damages.

The central issue in these cases was whether X's patent rights could be enforced as against Y's actions under the principle of territoriality, which holds that patent systems are governed by the laws of each country and that patent rights are recognized only within that country's territory. Specifically, in Case 1, the question was whether Y's distribution of programs from outside Japan to Japan via the Internet constituted "providing through telecommunications lines" (Article 2, Paragraph 3, Item 1 of the Patent Act). In Case 2, the issue was whether Y's act of constructing a system that includes a server outside Japan and a terminal in Japan by transmitting files via the Internet fell under "producing" as used in the Patent Act (Article 2, Paragraph 3, Item 1).

In Case 1, the Supreme Court noted that "in the modern age, when the distribution of information across national borders via telecommunications lines has become extremely easy, if the mere fact that a program is transmitted from outside Japan via a telecommunications line means that the patent right in Japan does not apply, and that the above provision does not fall under 'providing through telecommunications lines' (Article 2, Paragraph 3, Item 1 of the Patent Act), then... this is not in line with the purpose of the Patent Act, which is to contribute to the development of industry through the protection and encouragement of inventions." The court then considered the circumstances under which patent rights are effective, stating that "when the act in question is viewed as a whole and is assessed as effectively constituting 'providing through telecommunications lines' within Japan's territory, there is no reason to deny an interpretation that the patent rights of Japan are effective regarding that act."

The court pointed out that, although Y's distribution of programs could be seen as partly occurring outside

Japan, when viewed as a whole, it is naturally carried out when users in Japan access the web page to receive Y's service. This allows videos to be watched on terminals in Japan using the programs. The distribution by Y "is carried out as part of the information processing process when providing the respective services in Japan, and makes it possible to naturally achieve the effects of the respective program inventions on terminals located in Japan. The location of the server outside Japan is not particularly significant in this context." The court also highlighted the economic impact of Y's actions on X and concluded that Y was "effectively providing the respective programs via telecommunications lines within the territory of Japan" through the distribution, and thus recognized an infringement of the relevant patent rights.

In Case 2, the Supreme Court reached a similar conclusion, determining that Y was effectively "producing" in Japan and found that there had been an infringement of the patent rights.

As reported in Vol. 4 issue of this newsletter, the first instance courts in both cases applied a strict and formalistic territoriality principle and ruled against X, while the Intellectual Property High Court, in the second instance, took a flexible and substantial approach to territoriality and reversed the lower court, ruling in favor of X. The Supreme Court decision is a significant precedent, demonstrating that even if the act in question does not fully occur in Japan, the effect of the patent right may be enforceable against such acts based on the totality of the actual circumstances. It will be noteworthy to see how the scope of the Supreme Court's decision and the specific logic upon which it relies are applied in future court cases and wider industry debates.

6. Association for Countermeasures Against Dark Patterns Releases "Dark Pattern Countermeasures Guidelines ver1.0"

The Association for Countermeasures Against Dark Patterns plans to launch in July 2025 the NDD (Non-Deceptive Design) accreditation system, a system in which a neutral third party examines and certifies the websites of honest businesses that do not use dark patterns, and grants them a logo mark that cannot be tampered with. In order to operate the NDD accreditation system, this Association formulated and published the "Dark Pattern Countermeasures Guidelines ver1.0" on January 30, 2025. These guidelines, which were formulated based on discussions at a subcommittee meeting attended by the Consumer Affairs Agency, the Ministry of Internal Affairs and Communications, the Personal Information Protection Commission, and the

Ministry of Economy, Trade and Industry as observers, in addition to experts and general companies, indicate items subject to examination under the NDD accreditation system, and provide detailed explanations of non-dark pattern implementation and the organizational measures required of honest businesses.

In Japan, where there is no comprehensive law regulating dark patterns, this kind of voluntary effort on the private level is noteworthy. This Association is holding several online information sessions on these guidelines and the NDD accreditation system in March and April. The schedule, application procedures, and other details can be found on the Association's website.